引　言

代数 K-理论是环上(特别是域上)线性代数的推广与深化(尤其是处理"大矩阵"的极限情况,即对一个环 R,将 $A \in R^{n\times n}$ 视作 $\begin{pmatrix} A & \\ & I_\infty \end{pmatrix}$ 或 $\begin{pmatrix} A & \\ & O_\infty \end{pmatrix} \in R^{\infty\times\infty}$)。对一个环 R,代数 K-理论给出一系列 Abel 群 K_i,$i\in\mathbb{Z}$,作为环 R 的"不变量",是刻画环的先进工具之一。事实上,K_i 都是环范畴 $\mathcal{R}$ing 到 Abel 群范畴 $\mathcal{A}\mathcal{G}$ 的(共变)函子。在这些 K_i 群中最重要的是 K_0 群、K_1 群及 K_2 群,而最基本的是 K_0 群(可看作是域上线性空间维数理论的推广,它是由有限生成投射模范畴中元素的同构类定义的 Abel 群,本书中将给出三种等价的定义)。K_1 群可看作是环上可逆矩阵的行列式研究的深化,事实上是环上可逆矩阵群(一般线性群)在极限情况下的 Abel 化。而从范畴的角度上看,它又可由 K_0 群导出,至于 K_2 群则可看作是环上的初等矩阵群(在极限情况下)泛中心扩张的核。从同调的角度上看,K_1,K_2 群又都是相应群的同调群。对这些内容,本书中都给出详细的介绍。

代数 K-理论在代数数论、代数拓扑、代数几何及算子代数等学科中起着重要的作用。比如,代数数论中起源于 Fermat 大定理研究中的因子分解问题的代数数域(有理数域 $\mathbb{Q}$ 的有限扩张域)F 的类数计算,这事实上已归为 $K_0(O_F)$ 的研究,这里的 O_F 为 F 的代数整元环。作为五维以上流形分类的主要工具,拓扑学中的 Whitehead 挠(torsion),实质上是所研究的拓扑空间之基本群 π 的整群环 $\mathbb{Z}\pi$ 的 K_1 群 $K_1(\mathbb{Z}\pi)$ 的元素。在研究连通拓扑空间何时同伦等价于一个有限 CW-复形的问题中,1965 年 C. T. Wall 进一步地研究了由有限复形支配的拓扑空间 X(即 X 的奇异复形 $S(X)$ 链同伦等价于一个有限长的有限生成投射模的复形),他定义了广义 Euler 示性数(特征标)$\chi(X)\in K_0(\mathbb{Z}\pi)$,其中 π 为 X 的基本群。而通常的 Euler 示性数即 Betti 数(X 的系数在某一环 R 中的第 i 个同调群 $H_i(X;R)$ 之秩)的交错和。对广义 Euler 示性数,Wall 证明了:X 存在有限自由复形的同伦型等价于 $\chi(X)\in\mathbb{Z}$,即在约化 K_0 群 $\widetilde{K}_0(\mathbb{Z}\pi)$ 中 $\chi(X)$ 为 0,用拓扑语言来说,即

Wall 定义的有限性障碍(Obstruction)消失。现在 K_0 群也常称为 Grothendieck 群,是为了纪念在代数 K-理论中作出奠基性贡献的 Grothendieck。1957 年他关于代数几何中著名的 Riemann-Roch 定理的推广是他从事 K-理论工作的源泉。Riemann-Roch 定理给出了两个上同调空间的维数差公式,这些维数差都可在(一般)环的 K_0 群中对有限生成投射模得到优美的类比。对于群论,研究算术群(李群中带有算术性质的一类离散子群,如实数域中 $\mathbb{R}$ 的整数加群 $\mathbb{Z}$,$GL_n(\mathbb{R})$ 中的 $GL_n(\mathbb{Z})$,$SL_n(\mathbb{R})$ 中的 $SL_n(\mathbb{Z})$,或更一般地代数数域 F 中代数整元环 O_F 上的 $SL_n(O_F)$,$GL_n(O_F)$ 等都是,这里 GL_n 表 n 阶一般线性群(n 阶可逆矩阵群),SL_n 表特殊线性群(行列式为 1 的 GL_n 之子群)中是否每一个有限指数的子群都包含一个同余子群,即著名的同余子群问题(比如,对交换环 R 上的 $SL(R)\equiv\varinjlim SL_n(R)$。任取 $J\lhd R$,则称 $SL(R,J)\equiv\{A\in SL(R)\mid A\equiv I(\mathrm{mod}\ J)\}$ 为 $SL(R)$ 关于理想 J 的同余子群)。同余子群问题在单群分类中有重要的意义,它与 K_1 群的计算也是密切相关的。关于 K_2 群,目前在代数数论中计算或估计代数数域 F 之代数整元环 O_F 的 K_2 群,仍是热门的前沿课题之一,有大量的问题尚待研究。至于高阶 K 群(K_i 群,$i\geqslant 3$),尤其是域与整数环的高阶 K 群,因与 L-函数的特殊值有密切关系,因而能反映出数论中的一些信息,已受到数论研究者的重视。对于算子代数,代数 K-理论(尤其是 K_0 群与 K_1 群)已成为有力的工具之一。近期的成果十分丰富,二十世纪八十年代即已出现精彩的算子代数的 K-理论专著。

在二十世纪五十年代尚无代数 K-理论这一术语出现,第一本代数 K-理论专著[Bass,1968]是 H. Bass 在 1968 年完成的(R. S. Swan 1968 年的专著[Swan,1968]以 Bass 的书作参考文献),1978 年数学的 Fields 奖授于 1976 年解决 Serre 猜测的 D. Quillen 后,这一学科更加引人注目。1990 年之前在美国《数学评论》(Math. Rev.)与德国《数学文摘》(Zbl)的分类中,代数 K-理论还只是隶属于同调代数的小分支。1985 年作者在美访问时,不少同行告知,他们已强烈要求将代数 K-理论单列为大学科,在 1991 年,这两家权威杂志的分类(2000 年分类也是)中已将代数 K-理论列为与数论、复变函数、泛函分析、几何学、偏微分方程等并列的大学科)(19××)。由此也可看出代数 K-理论的发展速度与重要性。

代数 K-理论对拓扑学与几何学中的向量丛理论的应用特别引人注目。设 E,B 为两个拓扑空间,$p:E\to B$ 为连续(满)映射。$\forall b\in B$,原象 $p^{-1}(b)$

称为 p 在 b 上的纤维(fibre)，三元组 (E,p,B) 称为 B 上的一个丛(bundle)，B 称为此丛的基空间，E 称为此丛的全空间，p 则称为其丛投射。若又有连续映射 $s:B\to E$ 使 $ps=I_B$（B 上的恒同映射），则称 s 为此丛的一个截面(section)。一般地，截面未必存在，如二维球面 S^2 上不存在连续的切向量场。当丛 (E,p,B) 的每一个纤维都有某固定域 F 上的有限维向量空间结构且它们的维数连续（即 $\forall b\in B$，都有 b 的邻域 $U(b)$ 使 $U(b)$ 上的纤维都有同一维数（对 F-向量空间））时，(E, p, B) 又称为向量丛。1930年，这个概念首次出现在流形的拓扑与几何问题中。1950 年有较完美的形式与理论。1960 年，M. F. Atiyah 与 F. Hirzebruch 沿 Grothendieck 的研究方向作出了出色的工作，发展了这一理论。1955 年，J. P. Serre 得到了一个关键性的结果：仿射簇(affine variety)（代数曲线、代数曲面的抽象与概括）上的向量丛与此簇的坐标环上的有限生成投射模之间有一一对应的等价关系，后来，当域 $F=\mathbb{R},\mathbb{C}$（复数域）、$\mathbb{H}$（四元数体），以 $\mathrm{C}(X)$ 表示 X 到域 F 的连续函数环时，此结果被推进为：紧致 CW-复形 X 上的 F-向量丛范畴自然等价于 $\mathrm{C}(X)$ 上的有限生成投射模范畴。1962 年，R. W. Swan 又将此结果更进一步地推广为：当 $F=\mathbb{R},\mathbb{C}$ 时，紧致 Hausdorff 空间 X 上的 F-向量丛范畴自然等价于 $\mathrm{C}(X)$ 上的有限生成投射模范畴。由此建立了一座大桥，沟通了拓扑 K-理论与代数 K-理论的许多结果与方法。作为一个例子，我们来简述一下拓扑学中 K^0 群与代数 K-理论中的 K_0 群的一个优美关系。对 B 上的两个丛 $\xi_1=(E_1,p_1,B)$ 与 $\xi_2=(E_2,p_2,B)$ 定义它们的直和（也称 Whitney 和，纤维积）为 $\xi_1\oplus\xi_2=(E_1\oplus E_2,q,B)$，其中 $E_1\oplus E_2=\{(e_1,e_2)\mid p_1(e_1)=p_2(e_2),e_1\in E_1,e_2\in E_2\}$，$q(e_1,e_2)=p_1(e_1)(=p_2(e_2))$。对两个丛 (E,p,B) 与 (E',p',B')，其丛同态定义为 $(u,f):(E,p,B)\to(E',p',B')$，其中 $u:E\to E'$，$f:B\to B'$ 为使 $p'u=fp$ 的连续映射。

当 $B=B'$，$f=I_B$ 时 u 即 B 上丛范畴中的态射(morphism)，由此可定义丛同构。并用 $[E]$ 表示丛 (E,P,B) 所在的同构类。不难看出 $\oplus$ 对同构类诱导一个相容的运算（仍记为 $\oplus$，与代表元选取无关）。于是

$\mathcal{B}\mathrm{un}(B)=\{[E],\oplus\mid(E,p,B)$ 为丛$\}$，

$\mathcal{V}\mathrm{ec}(B)=\{[E],\oplus\mid(E,p,B)$ 为向量丛$\}$

都是 Abel 半群（且有零元素，因而又是带幺半群(monoid)）。在 §1 中我们将对每一个 Abel 半群进行“（群）完备化”得到同构意义下惟一的 Abel 群。将 $\mathcal{V}\mathrm{ec}(B)$ 的（群）完备化记为 $\mathrm{K}^0(B)$，将有限生成投射 $\mathrm{C}(B)$-模的同构类所

成的 Abel 半群的群完备化记为 $K_0(C(B))$。由上述的 Swan 的结果可知，当 B 为紧致 Hausdorff 空间时，$K^0(B)\simeq K_0(C(B))$(事实上还是环同构)。因此拓扑学中 K^0 群的计算常可归为代数计算。

本书是作者在南京大学近二十年讲稿的基础上写成，主要立足于介绍代数 K-理论及其应用的基础性内容，其中包含了作者及学生们在业师周伯埙先生指导下所得的部分结果，也包含着作者本人尚未发表的一些结果，前 12(或前 10)节可作为数学系硕士或博士研究生(或学习代数方向的高年级本科生)一学期讲课内容(对本科生必要时补一点投射模基础即可)。后 19(或后 21)节即可作为博士生进一步学习的内容。

从另一角度看，本书又是一本代数 K-理论的入门性专著。阅读本书的读者(只要求学过线性代数与近世代数)当有能力在各节中解答一些问题，比如补上未加详述的证明；从各节设立的一些注中找出研究性的问题；也可从自己熟悉的学科出发去找应用，或参考[Silvester,1981]与[Rosenberg,1994]等书中的习题进行练习。因此，为了不约束读者的思路，本书不再另设习题。此外，我们认为在阅读或学习本书之前读一下[周伯勋,1988]与[佟文廷,1998]将是有益的。

按照惯例，本书中的环均指有单位元的结合环，(左、右)环模均指酉模，本书的参考文献中，外语论文的作者按字典序排列。同一作者的论著将用作者(或第一作者)的姓(名)(而不是姓的第一字母)后加发表年代作序号按发表期排列，同一作者同一年发表的不同论著则在年代后再标下足码 1,2,…。中文作者的文献则按笔划序，这将会给读者带来方便。

定理、命题、推论与引理的编码中第一数字为其所在节数，第二个数字为在该节中的序号。比如定理 2.1 表示 §2 中的第 1 条定理，这样，读者在阅读后文用到前面的结果时是会感到方便的，因为本书中的节次(虽然分到各章)统一编号，无重复。

在本书中除(外国)人名及环类缩写字母外，凡是可作为函子(或与函子有密切联系)的字母也都用正体，以求醒目。为方便读者，本书后面列有常用符号表，以备读者查阅。

本书是在南京大学的支持与鼓励下完成并出版的。在本书稿的多年使用中，听课的研究生(如今已有十余位在教授岗工作，其中七位在博士生导师岗工作)提出了许多宝贵意见。这两年听课的研究生(欧阳柏玉，唐高华，周德旭，黎奇升，张良云，祝家贵，卢丹诚，吴俊，肖光世，陈卫星，张洪波，毛

立新，王永铎，石小平，张国印等）还对打印稿作了极为细心的校正，在此也一并致谢。

本书尽管经过了多年的努力，限于著者的水平，不妥之处，甚至错误之处，仍难以免除。敬请专家、学者以及本书的读者们不吝指正。

佟文廷

2003年5月于南京大学

目　录

第一章　K_0 群的基础理论

本章是 K_0 群的最基本的理论，主要是介绍 K_0 群的三种等价定义。第一种定义立足于半群的完备化，将环 R 的 K_0 群定义为有限生成投射(左)R-模同构类对加法所成的交换半群的(群)完备化，一个由 R 确定的 Abel 群；第二种定义立足于自由 Abel 群的商群；第三种定义则立足于在线性代数中早已为读者熟悉的幂等矩阵。我们证明了这三种定义的等价性以及 K_0 的函子性。作为应用，本章还介绍了一些 K_0 群结构或性质反映出的环性质。对不带单位元的环，也给出了 K_0 群的定义，并且证明了这种定义对有单位元环(本书中除特别声明外，所用到的环都指有单位元的结合环)使用所得的 K_0 群与上述的三种定义是一致的(同构的)。对概括广的重要环类——半局部环，在§3 中证明了半局部环的 K_0 群必为 $\mathbb{Z}^n$ 形的有限生成自由 Abel 群，同时给出了对群环的应用。在这一节中从 K_0 的函子性出发，又给出了一类 IBN 环(特别是交换环)以约化群作直和项的 K_0 群分解。在§2 中，用 K_0 的函子性还给出了多项式环及群环的 K_0 群的分解。在§4 中介绍交换环的局部化及有限生成投射模的局部秩，利用 K_0 群给出了环连通性及拓扑空间连通性方面的有意义的结果，更显示了 K_0 群的应用价值。

§1　环的 K_0 群(Grothendieck 群)

先从半群的(群)完备化谈起，以给出 K_0 群的第一种定义法。事实上，由非负整数加法半群 $\mathbb{N}$ 得到整数加群 $\mathbb{Z}$，或由乘法半群 $\mathbb{Z}^* = \mathbb{Z}\setminus\{0\}$ 得到有

理数乘法群 $\mathbb{Q}^*$ 都是半群完备化的结果。知道交换整环(无零因交换环)的分式域或更进一步地知道交换环局部化的读者将会看出,下面用到的方法实质上是构作分式域或局部化方法的特殊化(这里只牵扯到一种运算)。

设 S 为交换(加法)半群,但未必有单位元(零元)。在 $S\times S$ 上定义关系

$$(x,y)\sim(u,v)\Leftrightarrow \exists\ t\in S$$

使

$$x+v+t=y+u+t,\quad \forall x,y,u,v\in S$$

(当 S 为可消半群时,t 可省去)。显然,这是一种等价关系,记 $[(x,y)]$ 为 (x,y) 所在的等价类。并定义运算

$$[(x,y)]+[(x',y')]=[(x+x',y+y')],\forall x,y,x',y'\in S$$

不难看出,这是与上述等价关系相容(即与代表元选取无关)的且满足结合律与交换律的加法运算。同时

$$[(x,x)]=[(y,y)],\qquad \forall x,y\in S$$

即为此运算下的零元素(简记为 0)。于是由

$$[(x,y)]+[(y,x)]=[(x+y,x+y)]=0$$

知

$$[(x,y)]=-[(y,x)],\qquad \forall x,y\in S$$

这样,我们就由 S 得到一个加法 Abel 群,记为 $G=S\times S/\sim$。对 S 与 G 可定义一个标准的半群同态(建议读者自证:此标准同态为单同态 $\Leftrightarrow$ S 为可消半群)

$$\varphi\colon S\to G;\quad x\mapsto[(x+x,x)]$$

显然 φ 的象 $\mathrm{Im}\varphi$ 生成 G(记为 $\langle\varphi(S)\rangle=G$ 或 $\langle\mathrm{Im}\varphi\rangle=G$)。现在来证明标准同态 $\varphi:S\to G$ 或者说 (G,φ))有如下的泛性质(universal property),记为 $(G,\varphi)\in\mathrm{UP}$ 或简记为 $\varphi\in\mathrm{UP}$,有时也记为 $G\in\mathrm{UP}$。

UP:对任意的群 H 与任意的半群同态 $\psi:S\to H$,$\exists$(存在惟一)群同态 $\theta:G\to H$ 使右图为交换图:

$$\begin{array}{ccc} S & \xrightarrow{\varphi} & G \\ {\scriptstyle\forall\psi}\downarrow & \swarrow{\scriptstyle\theta\ \exists 1} & \\ \forall H & & \end{array}$$

即 $\theta\varphi=\psi$(用范畴语言来说,即 $S\xrightarrow{\varphi}G$ 为范畴 $\{S\xrightarrow{\psi}H\mid H$ 为群,ψ 为半群同态$\}$(其中的态射用交换图常规地定义))中的始对象。

事实上,定义 $\theta([(x,y)])=\psi(x)-\psi(y)$,$\forall x,y\in S$,可直接验知 θ 为群同态且

$$\theta\varphi(x)=\theta([(x+x,x)])$$

$$= \psi(x+x) - \psi(x) = \psi(x), \forall x \in S$$

因此 $\theta\varphi=\psi$。而 θ 的惟一性则由 $G=\langle \mathrm{Im}\varphi \rangle$ 即知，于是我们可得：

引理 1.1（交换半群完备化(completion)定理） 设 S 为交换(加法)半群(未必有零元)，则

(1) 有 Abel 群 G(S 的完备化，也称为 S 的 Grothendieck 群，常记为 $G(S)$)与半群同态 $\varphi:S\to G$ 使 $\varphi\in \mathrm{UP}$(即具有上述的泛性质)；

(2) 在同构意义下，(G,φ)是惟一的，即若又有 $\varphi':S\to G'$ 使 $\varphi'\in\mathrm{UP}$，则有群同构 $\alpha:G\to G'$ 使右图为交换图，即 $\varphi'=\alpha\varphi$。

$$\begin{array}{ccc} S & \xrightarrow{\varphi} & G \\ {\scriptstyle\varphi'}\downarrow & \swarrow{\scriptstyle\alpha,\ \exists 1} & \\ G' & & \end{array}$$

证 由前段构作与说明知，这里只需证(2)。下面用常规证法(凡是具有某类泛性质的对象，若存在，都可用此法证其(同构意义下的)惟一性)。

由$(G,\varphi)\in\mathrm{UP}$ 知同态 $\alpha:G\to G'$存在，使 $\varphi'=\alpha\varphi$。由$(G',\varphi')\in\mathrm{UP}$ 知同态 $\beta:G'\to G$ 存在，使 $\varphi=\beta\varphi'$，于是有 $\beta\alpha\varphi=\varphi$。但取 $H=G,\psi=\varphi$，由上知存在惟一的 $\theta:G\to G$ 使 $\varphi=\theta\varphi$。另一方面，显然恒同同态 $I_G:G\to G$ 也使 $\varphi=I_G\varphi$。于是由上知 $I_G=\theta=\beta\alpha$。同理知 $\beta\alpha=I_{G'}$。故 α 为同构。 □

注① 若在环 R 的定义中只要求 R 对加法为交换半群(有零元时，是幺半群)，则称 R 为半环(semiring)，仿前再定义乘法为(将$[(a,b)]$视作 $a-b$ 容易理解此定义)

$$[(x,y)][(x',y')]=[(xx'+yy',xy'+yx')], \forall x,y,x',y'\in R$$

即得半环的完备化，在纤维丛理论中常会用到。

下面对一般的环 R，记 f. g. $\mathrm{P}_R\mathfrak{M}$ 为有限生成投射(左)R-模范畴，且记集合

$$\mathrm{Proj}(R)=\{\langle X\rangle(X\text{ 的同构类})\mid X\in \text{f. g. }\mathrm{P}_R\mathfrak{M}\}$$

再定义运算

$$\langle X\rangle+\langle Y\rangle=\langle X\oplus Y\rangle,\qquad \forall X,Y\in \text{f. g. }\mathrm{P}_R\mathfrak{M}$$

则易见 $\mathrm{Proj}(R)$为交换半群(且有零元 0)。于是有 K$_0$ 群的第一种定义法：

定义 1.1 设 R 为任意环，称交换半群 $\mathrm{Proj}(R)$的完备化为 R 的 K$_0$ 群(也称为 R 的 Grothendieck 群)，记为 $\mathrm{K}_0(R)$或 K_0R，即 $\mathrm{K}_0(R)=G(\mathrm{Proj}(R))$。

值得注意的是，前面已要求读者证明：对交换半群 S，标准同态 $\varphi:S\to G(S)$为单同态的充要条件是 S 为可消半群。而 $\mathrm{Proj}(R)$通常都不是可消半群，因此 $\varphi:\mathrm{Proj}(R)\to\mathrm{K}_0(R)$通常都不是单同态。这里牵扯到一个著名的难题——模的直和消去问题(即由模同构 $M\oplus A\simeq N\oplus A$ 何时蕴含着 $M\simeq$

N 的问题)，这也是近二十年来的一个重要热门课题，但所得结果离人们期望的相差甚远。值得一提的是 1993 年 R. Camps 与 W. Dicks 在[Camps，1993]中证明了：一切 Artin 模都可在直和中消去。这是一个十分引人注目的结果，由此可推出对 Artin 环 R，Proj(R)是可消的。在模的直和消去问题中，武同锁在他(1994 年)的博士论文中定义了环的弱稳定度等概念，在此基础上给出了一系列有价值的结果(后已整理成论文数篇在国内外发表，见[武同锁，1994]等)。

现在再给出 K_0 群的第二种定义法。

对任意环 R，取 $\mathscr{F}=\mathscr{F}(R)$ 为以 Proj(R)的全体元素作基的自由 Abel 群，记

$$\mathscr{R}=\langle\{\langle P\rangle+\langle Q\rangle-\langle P\oplus Q\rangle \mid P,Q\in \text{f. g. } \mathrm{P}_R\mathfrak{M}\}\rangle$$

(注意，这里的 $\langle P\rangle+\langle Q\rangle-\langle P\oplus Q\rangle$ 是 $\mathscr{F}$ 中的运算，而非 Proj(R)中的运算，因此一般地并不等于 0)。显然 $\mathscr{R}$ 为 $\mathscr{F}$ 的正规子群，因此商群 $\mathscr{F}/\mathscr{R}$ 存在(惟一)，将标准同态 $\pi:\mathscr{F}\to\mathscr{F}/\mathscr{R}$ 下 $\langle P\rangle$ 的象记为 $[P]$，即 $\pi(\langle P\rangle)=[P]$。我们证明下述的定理 1.1 后即看到：取 $\mathscr{F}/\mathscr{R}$ 为 R 的 K_0 群即给出与第一种定义法等价的定义(定理 1.1 中的 $\mathrm{K}_0(R)$暂且表示第一种定义给出的 R 之 K_0 群)。

定理 1.1 对任意环 R，

$$\mathrm{K}_0(R)\simeq\mathscr{F}/\mathscr{R}=\langle\{[P]=\overline{\langle P\rangle}(\mathrm{mod}\ \mathscr{R}) \mid P\in \text{f. g. } \mathrm{P}_R\mathfrak{M}\}\rangle$$

即 $\mathrm{G}(\mathrm{Proj}(R))\simeq\mathscr{F}/\mathscr{R}$。

证 由 $\mathscr{F}$，$\mathscr{R}$ 的构作知，$\mathscr{F}/\mathscr{R}$ 中显然有

$$[P\oplus Q]=[P]+[Q],\qquad \forall P,Q\in \text{f. g. } \mathrm{P}_R\mathfrak{M} \tag{1}$$

由此合并 $\mathscr{F}/\mathscr{R}$ 各元素中形式上的正、负项知

$$\mathscr{F}/\mathscr{R}=\{[P]-[Q] \mid P,Q\in \text{f. g. } \mathrm{P}_R\mathfrak{M}\} \tag{2}$$

而

$$\mathrm{K}_0(R)=G(\mathrm{Proj}(R))=\{[(\langle P\rangle,\langle Q\rangle)] \mid P,Q\in \text{f. g. } \mathrm{P}_R\mathfrak{M}\}$$

于是定义映射

$$\theta:\mathrm{K}_0(R)\to\mathscr{F}/\mathscr{R}$$
$$[(\langle P\rangle,\langle Q\rangle)]\mapsto[P]-[Q]$$

容易看出 θ 为满映射，且为群同态。又可证 θ 为单射，因此为群同构。 □

按定理 1.1，今后我们不再区分 $\mathrm{G}(\mathrm{Proj}(R))$与 $\mathscr{F}/\mathscr{R}$，统一记为 $\mathrm{K}_0(R)$，从而有：

命题 1.1 对任意环 R，

$$\mathrm{K}_0(R)=\{[P]-[Q] \mid P,Q\in \text{f. g. } \mathrm{P}_R\mathfrak{M}\}$$
$$=\{[P_1]-[R^n] \mid P_1\in \text{f. g. } \mathrm{P}_R\mathfrak{M},n\in\ \}$$

$$=\{[P_1]-n[R]\mid P_1\in \text{f. g. P}_R\mathfrak{M}, n\in \mathbb{N}\}$$

证　由定理 1.1 之证中的(1),(2)知,只需证第二等式。

事实上,由 $Q\in$ f. g. $\text{P}_R\mathfrak{M}$ 知可设 $Q\oplus Q_1\simeq R^n$,于是有

$$\begin{aligned}[P]-[Q]&=[P]+[Q_1]-([Q]+[Q_1])\\&=[P\oplus Q_1]-[R^n]\end{aligned}$$

取 $P_1=P\oplus Q_1$ 即得欲证。　□

对于 $K_0(R)$ 中的元素我们有揭示其相等本质的如下结果:

命题 1.2　对任意环 R,在 $K_0(R)$ 中

$$[P]=[Q]\Leftrightarrow \exists n\in \mathbb{N} \text{ 使 } P\oplus R^n\simeq Q\oplus R^n$$

此时称 P,Q 为**稳定同构的(准同构的**(stably isomorphic)),记为 $P\overset{s}{\simeq}Q$。

证　$\Rightarrow$:$[P]=[Q]$即$[P]-[Q]=0$,按第一种定义这也等价于$[(\langle P\rangle,\langle Q\rangle)]=0=[(\langle 0\rangle,\langle 0\rangle)]$,即$\exists T\in$ f. g. $\text{P}_R\mathfrak{M}$ 使(在 Proj(R)中)

$$\langle P\rangle+\langle 0\rangle+\langle T\rangle=\langle Q\rangle+\langle 0\rangle+\langle T\rangle$$

即

$$P\oplus T\simeq Q\oplus T$$

令 $T\oplus T_1\simeq R^n$,即得 $P\oplus R^n\simeq Q\oplus R^n$。

$\Leftarrow$:若 $P\overset{s}{\simeq}Q$,即有 $n\in\mathbb{N}$ 使 $P\oplus R^n\simeq Q\oplus R^n$,则

$$[P]+[R^n]=[Q]+[R^n]$$

因此$[P]=[Q]$。　□

由上证可得:

推论 1.1　$\forall P,Q\in$ f. g. $\text{P}_R\mathfrak{M}$,$P\overset{s}{\simeq}Q\Leftrightarrow \exists T\in$ f. g. $\text{P}_R\mathfrak{M}$ 使 $P\oplus T\simeq Q\oplus T$。

值得注意的是:

$$\text{同构}\ \underset{\not\Longleftarrow}{\Longrightarrow}\ \text{稳定同构}$$

(见后面的例 1)

这说明即使在 f. g. $\text{P}_R\mathfrak{M}$ 中有限生成投射模,甚至有限生成自由模,也未必可从直和中消去(在向量丛范畴 Vec(X)中对应地有:向量丛,甚至平凡丛未必可从直和中消去)。因此直和消去问题与稳定同构何时为同构的问题是密切相关的。对一些特殊的环类可得到比较显见的结果。比如,当 R 为域,更一般地为除环时 f. g. $\text{P}_R\mathfrak{M}=$ f. g. $\text{Free}_R\mathfrak{M}$(有限生成自由 R-模范畴。在这里即有限维线性 R-空间范畴)。因此

$$P\simeq Q\Leftrightarrow \dim P=\dim Q,\qquad \forall P,Q\in \text{f. g. P}_R\mathfrak{M}$$

当 R 为 PID(主理想整环(类),记为 $R\in$ PID,比如 $\mathbb{Z}\in$ PID,域 F 上的一元多项式环 $F[X]\in$ PID)时,自由模的子模仍是自由的。因此 f. g. $\mathrm{P}_R\mathfrak{M}$ = f. g. $\mathrm{Free}_R\mathfrak{M}$ 也成立,再注意到 PID$\subset$IBN(不变基数环类,$R\in$ IBN 即指 $R^m\simeq R^n$ 时必有 $m=n$。如交换环,左(右)Noether 环都是 IBN 环),此时稳定同构即同构。因此(暂将下面的 rank 视作 dim, 即 $\mathrm{rank}P=n \Longleftrightarrow P\simeq R^n$)

$$P \overset{S}{\simeq} Q \Leftrightarrow P \simeq Q \Leftrightarrow \mathrm{rank}P = \mathrm{rank}Q$$

当 R 为局部环时,由于投射 R-模都是自由 R-模,且局部环也是 IBN 环,此时这一结果仍成立。对上述这些环类的 R,将 $P\in$ f. g. $\mathrm{P}_R\mathfrak{M}$ 的稳定同构类 $[P]$ 对应着 $\mathrm{rank}P$,由(1)式与

$$\mathrm{rank}(P \oplus Q) = \mathrm{rank}P + \mathrm{rank}Q$$

得下述的有用结果。

定理 1.2 设 R 为 PID(比如为域,除环)或局部环(未必是交换环),则

(1) $\mathrm{K}_0(R)\simeq\mathbb{Z}$(作为 Abel 群);

(2) 在 f. g. $\mathrm{P}_R\mathfrak{M}$ 中稳定同构即同构;

(3) 在 f. g. $\mathrm{P}_R\mathfrak{M}$ 中直和消去律成立。

1976 年美国数学家 D. Quillen 与前苏联数学家 A. Suslin 独立地解决了 Serre 问题(见[Quillen,1976]与[Suslin,1976],他们证明了:对 PID 环上的 n 元多项式环 R,f. g. $\mathrm{P}_R\mathfrak{M}$ = f. g. $\mathrm{Free}_R\mathfrak{M}$。在这之后,众多数学家(比如见[Swan,1990])都认为这方面更深入的问题仍有很大的研究价值。1986 年我们在[佟文廷,1986]中定义了 PF 环的概念,即称使 f. g. $\mathrm{P}_R\mathfrak{M}$ = f. g. $\mathrm{Free}_R\mathfrak{M}$ 的环 R 为 **PF 环**。在此基础上已有不少研究成果出现(比如[佟文廷,1989],[Tong,1994],[Chen, 1995,1996]及[Liu ,2000]等),对 PF 环显然仿上可得如下推广:

定理 1.2′ 设 $R\in$ IBN$\cap$PF,则定理 1.2 中的(1),(2),(3)成立。

此外可证:对 Dedekind(整)环,定理 1.2 中的(2),(3)仍成立(见[Berrick,2000])。

下面举一个例子说明定理 1.2 中的(1),(2),(3)对一般的环未必成立。

例 1 设 F 为域,V 为 F 上的(可数)无穷维线性空间,则 $R=\mathrm{Hom}_F(V,V)$为环,由 $V\oplus V\simeq V$ 知,作为左 R-模

$$\begin{aligned} R \oplus R &= \mathrm{Hom}_F(V,V) \oplus \mathrm{Hom}_F(V,V) \\ &\simeq \mathrm{Hom}_F(V \oplus V,V) \simeq \mathrm{Hom}_F(V,V) \simeq R \end{aligned}$$

于是 $R \overset{S}{\simeq} 0$,但显然 $R\not\simeq 0$。因此,对这个环 R,定理 1.2 中的(2),(3)都不成立且 $R\notin$ IBN。

下面再证定理 1.2 中的(1)也不成立。事实上，我们可证 $\mathrm{K}_0(R)=0$。

由 $R\oplus R\simeq R\in{}_R\mathfrak{M}$ 知 $[R]+[R]=[R]$（在 $\mathrm{K}_0(R)$ 中），因此 $[R]=0$ 且更一般地 $[R^m]=0$，$\forall m\in\mathbb{N}$。

任取 $P\in\mathrm{f.g.P}_R\mathfrak{M}$，则有 $n\in\mathbb{N}$ 与 $Q\in\mathrm{f.g.P}_R\mathfrak{M}$ 使

$$P\oplus Q\simeq R^n\simeq R$$

于是可认为 $P\oplus Q=R$。因此有正交幂等元 $p,q\in R$（即 $p^2=p,q^2=q,pq=qp=0$）使 $P=Rp,Q=Rq$ 且 $R=Rp\oplus Rq$。由此易知，作为左 R-模，

$$V=RV=pV\oplus qV$$

这也是 F-线性空间的直和分解。因此由 $\dim_F V=\infty$ 知，不失一般地可设 $\dim_F pV=\infty$，即 $pV\simeq V$（作为 F-线性空间），于是有 $\mathrm{Hom}_F(pV,V)\simeq R$（作为左 R-模）。注意 P 中元素均可表为 rp，$r\in R$ 而 $rp(pv)=rp(v)$ $\forall v\in V$（即 $rp:pV\to V$ 为 $rp:V\to V$ 在 pV 上的限制），因此有单的左 R-模同态 $P\xrightarrow{i}\mathrm{Hom}_F(pV,V)\simeq R$。使 $i(rp)(v)=rp(pv)$，$\forall v\in V$。下面再证 i 为满同态即知 i 为同构：$P\overset{i}{\simeq}R$，因此 $[P]=0$。

事实上，任取 $\alpha\in\mathrm{Hom}_F(pV,V)$，对 $\forall v\in V$ 定义 $r_1:v\mapsto\alpha(pv)$，则 $r_1\in\mathrm{Hom}_F(pV,V)=R$。注意

$$r_1(qv)=\alpha(pqv)=0,\qquad \forall v\in V$$

蕴含着 $r_1q=0$。因此 $r_1=r_1p+r_1q=r_1p\in P$，即 $r_1\in P$ 且

$$r_1(v)=r_1(pv)=\alpha(pv),\qquad \forall v\in V(\text{即 } r_1|_{pV}=\alpha)$$

即 $i(r_1)=\alpha$，于是 i 为同构且 $[P]=0$。而由 $[R]=[P]+[Q]$ 知 $[Q]=0$，故 $\mathrm{K}_0(R)=0$。这是非 IBN 环的一个具体例子。

显然对任意 $R\notin\mathrm{IBN}$ 都有 $m>n$，使 $(m-n)[R]=0$。因此在 $\mathrm{K}_0(R)$ 中 $\mathrm{Ord}[R]<\infty$，反之，若 $\mathrm{Ord}[R]=t<\infty$，则有 $[R^t]=0$，于是有 $0<s\in\mathbb{N}$ 使 $t+s>0$ 且 $R^{t+s}\simeq R^t$，即 $R\notin\mathrm{IBN}$。于是有：

命题 1.3　$R\in\mathrm{IBN}\Leftrightarrow$ 在 $\mathrm{K}_0(R)$ 中 $\mathrm{Ord}[R]=\infty$

由此命题可看出：$R\in\mathrm{IBN}$（比如 R 为交换环）时，$\mathrm{K}_0(R)$ 必有同构于 $\mathbb{Z}$ 的子群。在§3 中我们将对交换环 R 进一步地证明 $\mathrm{K}_0(R)$ 必有同构于 $\mathbb{Z}$ 的直和项。

现在我们用下一命题说明对交换环 R，$\mathrm{K}_0(R)$ 也是一个交换环。

命题 1.4　设 R 为交换环，则 $\mathrm{K}_0(R)$ 在

$$[P][Q]=[P\otimes_R Q],\qquad \forall P,Q\in\mathrm{f.g.P}_R\mathfrak{M}$$

作为乘法时为交换环，且 $[R]=1$（单位元）。

证　任取 $P,Q\in\mathrm{f.g.P}_R\mathfrak{M}$，则有 $m,n\in\mathbb{N}$ 与 $P_1,Q_1\in\mathrm{f.g.P}_R\mathfrak{M}$，使 $P\oplus$

$P_1 \simeq R^m$，$Q \oplus Q_1 \simeq R^n$ 于是由

$$R^{mn} \simeq R^m \otimes R^n \simeq (P \oplus P_1) \otimes (Q \oplus Q_1)$$
$$\simeq P \otimes Q \oplus \{(P \otimes Q_1) \oplus (P_1 \otimes Q) \oplus (P_1 \otimes Q_1)\}$$

知 $P \otimes Q \in$ f. g. $P_R\mathfrak{M}$。

又若 $P \overset{s}{\simeq} P'$，$Q \overset{s}{\simeq} Q'$（即$[P]=[P']$，$[Q]=[Q']$），则易验知$[P \otimes Q]=[P' \otimes Q']$，于是$[P][Q]=[P \otimes Q]$的定义与稳定同构类的代表元选取无关。再从$\otimes$在同构意义下的分配律与结合律即知 $K_0(R)$在上述运算下为交换环（注意 $P \otimes Q \simeq Q \otimes P$），而由 $R \otimes P \simeq P$，$\forall P \in$ f. g. $P_R\mathfrak{M}$ 知此环的单位元为$[R]$。 □

由命题 1.2 与命题 1.4 立得：

推论 1.2 设 $R \in$ PID（比如 R 为域）或 R 为交换局部环，则有环同构 $K_0(R) \simeq \mathbb{Z}$。

注② 有限生成理想都是主理想的整环称为 Bezout 环，半遗传（有限生成理想都为投射模的环称为半遗传环，见[佟，1998]）整环称为 Prüfer 环。显然

$$\text{PID} \subset \text{Bezout 环} \subset \text{Prüfer 环}$$

可以证明：若 R 为 Bezout 环，则 $K_0(R) \simeq K_0(R[x_1, \cdots, x_n]) \simeq \mathbb{Z}$ 且 R 与 $R[x_1, \cdots, x_n]$都为 PF 环。此外，若已知 R 为 Prüfer 环，则 $K_0(R) \simeq \mathbb{Z} \Leftrightarrow R$ 为 Bezout 环。尽管此结果很像 Dedekind 环中 R，$K_0(R) \simeq \mathbb{Z} \Leftrightarrow R \in$ PID，但 PID 与 Bezout 环仍是不同的概念。比如复数域 $\mathbb{C}$ 上的代数整数环为 Bezout 环，但非 PID。（见[McDonald，1984]）。

下面我们证明与 Euler 示性数有关的命题。

命题 1.5 设 R 为任意环，且有 f. g. $P_R\mathfrak{M}$ 正合列

$$0 \to P_n \xrightarrow{d_n} P_{n-1} \to \cdots \to P_1 \xrightarrow{d_1} P_0 \to 0,$$

则在 $K_0(R)$中，$\sum\limits_{i=0}^{n}(-1)^i[P_i] = 0$。

证 记 $K_i = \mathrm{Ker} d_i$，由设知有如下短正合列

$$0 \to K_1 \to P_1 \to P_0 \to 0,$$
$$0 \to K_i \to P_i \to K_{i-1} \to 0, \qquad i = 2, \cdots, n-1$$
$$0 \to P_n \to P_{n-1} \to K_{n-2} \to 0。$$

由 P_0 的投射性知 $P_1 \simeq K_1 \oplus P_0$，因此 $K_1 \in$ f. g. $P_R\mathfrak{M}$，由此知

$$[P_1] = [K_1] + [P_0]$$

用归纳法知 $K_{i-1} \in$ f. g. $P_R\mathfrak{M}$ 且 $P_i \simeq K_i \oplus K_{i-1}$，因此$[P_i]=[K_i]+[K_{i-1}]$，

$[P_{n-1}]=[P_n]+[K_{n-2}]$依次代入即得 $\sum_{i=0}^{n}(-1)^i[P_i]=0$。□

注③　设 $R\in \mathrm{IBN}$，$M\in \mathrm{FFR}$，即有 M 的有限长的有限自由分解

$$0\to F_n\to\cdots\to F_0\to M\to 0,\qquad \forall F_i\in \text{f. g. Free}_R\mathfrak{M}$$

可定义 M 的 Euler 示性数

$$\chi(M)=\sum_{i=0}^{n}(-1)^i\operatorname{rank}F_i$$

更一般地，对有限长的有限投射模复形（称为有限投射模复形）$(C,d)=(\{C_i\},d)(C_i\in \text{f. g. P}_R\mathfrak{M})$可定义其 Euler 示性数

$$\chi(C)=\sum(-1)^i[C_i]\qquad\text{（有限和）}$$

因此 $K_0(R)$与 Euler 示性数有密切关系（见[佟文廷，1989]）。

为了刻画 $K_0(R)\simeq\mathbb{Z}$ 的环 R。我们再引进如下定义：

定义 1.2　设 R 为任意环，$P\in \text{f. g. P}_R\mathfrak{M}$，若有 $m\in\mathbb{N}$ 使 $P\oplus R^m\in \text{Free}_R\mathfrak{M}$，（即有 $0\leqslant m<\infty$，$0<n<\infty$使 $P\oplus R^m\simeq R^n$），则称 P 为**稳定自由的（准自由的**（stably free）），记为 $P\in \mathrm{SF}_R\mathfrak{M}$。

若 $\text{f. g. P}_R\mathfrak{M}=\mathrm{SF}_R\mathfrak{M}$，即一切有限生成投射左 R-模都是稳定自由的，则称 R 为 PSF 环，记为 $R\in \mathrm{PSF}$。若 $\mathrm{SF}_R\mathfrak{M}=\text{f. g. Free}_R\mathfrak{M}$，则称 R 为 SFF 环记为 $R\in\mathrm{SFF}$（见[佟文廷，1986]）。对右 R-模可类似地定义 PSF 环与 SFF 环。

显然有

$$\text{f. g. Free}_R\mathfrak{M}\subseteq \mathrm{SF}_R\mathfrak{M}\subseteq \text{f. g. P}_R\mathfrak{M}$$

于是我们可将解决 Serre 猜测的 Quillen-Suslin 定理的广义研究归之为 PF 环即 PSF 环与 SFF 环的研究。因为显然有

$$\mathrm{PF}=\mathrm{PSF}\cap\mathrm{SFF}$$

现已知 SFF=UCP（见[Lam，1978]）（幺模列都可作为环 R 上的一可逆方阵的一列时 R 称为 UCP 环），因此这方面研究又归为 PSF 环的研究。

注④　定义 1.2 中条件"f. g.（有限生成）"及"$m<\infty$"都是必要的，否则将会导致平庸的定义（引不出新模类）。事实上，1972 年 M. R. Gabel 在其博士论文中已证（见[Lam，1978]）：若 $P\notin \text{f. g. }_R\mathfrak{M}$ 但有 $m\in\mathbb{N}$ 使 $P\oplus R^m\in \text{Free}_R\mathfrak{M}$，则 $P\in \text{Free}_R\mathfrak{M}$，又 S. Eilenberg 证出：若 $P\in \text{f. g. P}_R\mathfrak{M}$，则必有 $m=\infty$使 $P\oplus R^\infty\in \text{Free}_R\mathfrak{M}$。这只要令 $P\oplus Q\simeq E\in \text{f. g. Free}_R\mathfrak{M}$，由

$$P\oplus(Q\oplus P)\oplus(Q\oplus P)\oplus\cdots\simeq(P\oplus Q)\oplus(P\oplus Q)\oplus\cdots$$
$$\simeq E^\infty\in \text{Free}_R\mathfrak{M}$$

即知。

现来刻画使 $K_0(R)\simeq\mathbb{Z}$ 的环 R。即证：

命题 1.6 (1) 对任意环 R，$P\in \mathrm{SF}_R\,\mathfrak{M} \Leftrightarrow [P]\in \mathbb{Z}[R]$；

(2) 对任意环 R，$\mathrm{K}_0(R)=\mathbb{Z}[R]\Leftrightarrow P\in \mathrm{PSF}$（即 $\mathrm{SF}_R\,\mathfrak{M}=\mathrm{f.\,g.\,P}_R\mathfrak{M}$）；

(3) 设 R 为交换环，则有环同构 $\mathrm{K}_0(R)\simeq\mathbb{Z}\Leftrightarrow R\in \mathrm{PSF}$。

证 显然只需证(1)。因为(1)⇒(2)，(3)是显见的。

设 $P\in \mathrm{SF}_R\,\mathfrak{M}$，即有 $m,n\in\mathbb{N}$ 使 $P\oplus R^m\simeq R^n$。于是在 $\mathrm{K}_0(R)$ 中

$$[P]=[R^n]-[R^m]=(n-m)[R]\in\mathbb{Z}[R]$$

反之，设 $[P]=t[R]$，$t\in\mathbb{Z}$。则有 $s\in\mathbb{N}$ 使 $t+s>0$。于是

$$[P\oplus R^s]=(t+s)[R]=[R^{t+s}]$$

故由命题 1.2 知有 n 使

$$P\oplus R^s\oplus R^n\simeq R^{t+s+n}$$

即 $P\in \mathrm{SF}_R\,\mathfrak{M}$。 □

更一般地，我们有（见[佟文廷，1986]）：

命题 1.7 $R\in \mathrm{IBN}\cap \mathrm{PSF}\Leftrightarrow \mathrm{K}_0(R)\overset{f}{\simeq}\mathbb{Z}$ 且使 $f([R])=1$。（在 R 为交换环时 f 为环同构。）

证 ⇒：由 $R\in \mathrm{IBN}$ 知，$\forall n\in\mathbb{N}$，$\mathrm{rank}R^n=n$ 是惟一确定的，而由 $R\in \mathrm{PSF}$ 知，$\forall P\in \mathrm{f.\,g.\,P}_R\mathfrak{M}$，$P\in \mathrm{SF}_R\mathfrak{M}$，即有 $m,n\in\mathbb{N}$ 使 $P\oplus R^m\simeq R^n$。定义 $\mathrm{rank}P=n-m$。又 $P\overset{s}{\simeq}Q$，即有 $t\in\mathbb{N}$ 使 $P\oplus R^t\simeq Q\oplus R^t$，因此 $\mathrm{rank}P=\mathrm{rank}Q$（注意，$P,Q\in \mathrm{f.\,g.\,P}_R\mathfrak{M}$）。于是定义

$$f:\ \mathrm{K}_0(R)\to\mathbb{Z}$$
$$[P]\mapsto \mathrm{rank}P$$

即得（Abel）群同构且使 $f([R])=1$。

⇐：设 f 为群同构且 $f([R])=1$，则 $R^m\simeq R^n\Leftrightarrow m=n$。于是 $R\in \mathrm{IBN}$。又 $\forall P\in \mathrm{f.\,g.\,P}_R\mathfrak{M}$，由 $f([P])=t\in\mathbb{Z}$ 知必有 $s_1\in\mathbb{N}$ 使

$$f[P\oplus R^{s_1}]=f[R^{t+s_1}]=t+s_1>0$$

但 f 为群同构，因此 $[P\oplus R^{s_1}]=[R^{t+s_1}]$，即 $P\oplus R^{s_1}\overset{s}{\simeq}R^{t+s_1}$，这就证出了 $P\in \mathrm{SF}_R\,\mathfrak{M}$。 □

注⑤ 注意 R 为局部环或 PID 时，当然有 $R\in \mathrm{IBN}\cap \mathrm{PSF}$。又由 Quillen-Suslin 定理知 PID 上多元多项式环为 IBN 且为 PSF 环，于是由命题 1.7 我们又一次看出这些环的 K_0 群都同构于 $\mathbb{Z}$。

对于上面定义的 FFR 与 $\mathrm{SF}_R\,\mathfrak{M}$，我们可得一个有用的结果：

命题 1.8 对任意环 R，$\mathrm{f.\,g.\,P}_R\mathfrak{M}\cap \mathrm{FFR}=\mathrm{SF}_R\,\mathfrak{M}$。即，稳定自由模恰为有 FFR 的有限生成投射模。

证 由命题 1.5 与命题 1.6(1)即得。 □

§2 K_0 群的幂等阵定义与 K_0 的函子性

在本节中我们介绍环的 K_0 群的第三种定义法(第一、二种定义法见§1),我们将会看到:多一种定义法即多一个方便的工具。

设 $P\in$ f. g. $P_R\mathfrak{M}$,则在同构意义下可以认为有 $P_1\in{}_R\mathfrak{M}$ 使 $P\oplus P_1=R^m$ 且可以认为 $R^m=R^{m\times 1}$(R 上的 m 元列向量所成的 R-模)。记

$$p: R^m(=P\oplus P_1)\to P,\quad (x,y)\longmapsto (x,0)$$

则 $p^2=p\in R^{m\times m}$ 为幂等阵且 $p|_P=I_P$, $pR^m=P=\mathrm{Im}p$。对 $P\oplus P_1=R^m$ 两边取无穷直和,则又有 $P\oplus R^\infty=R^\infty$。因此也可认为上述的 p 为

$$R^{\infty\times\infty}\equiv\left\{\begin{pmatrix}p & \\ & 0_\infty\end{pmatrix}\middle|\ \exists m\in\mathbb{N}\text{ 使 } p\in R^{m\times m}\right\}$$

中的幂等阵(即不区分 p 与 $\begin{pmatrix}p & \\ & 0_\infty\end{pmatrix}$)且与 P 是一一对应的。类似地若 $Q\in$ f. g. $P_R\mathfrak{M}$,可令 $Q\oplus Q_1=R^n$ 则有幂等阵 $q\in R^{n\times n}$,使 $Q=\mathrm{Im}q=qR^n$,也可以认为 $q^2=q=\begin{pmatrix}q & \\ & 0\end{pmatrix}\in R^{\infty\times\infty}$。于是,$P$、$Q$ 分别对应 $R^{\infty\times\infty}$ 中的幂等阵 p、q,$P\oplus Q$ 则对应 $R^{\infty\times\infty}$ 中的幂等阵 $p\oplus q=\begin{pmatrix}p & & \\ & q & \\ & & 0_\infty\end{pmatrix}$。下面来定义与此运算相容的幂等阵的一种等价关系,为此先证明如下引理:

引理 2.1 对任意环 R,设 $P,Q\in$ f. g. $P_R\mathfrak{M}$ 各对应 $p^2=p\in R^{m\times m}$,$q^2=q\in R^{n\times n}$,则下述三点是等价的:

(1) $P\simeq Q$(作为左 R-模);

(2) 有 $x,y\in R^{\infty\times\infty}$,使 $p=xy$,$q=yx$(对称分解);

(3) 有 $u\in\mathrm{GL}(R)\equiv\left\{\begin{pmatrix}w & \\ & I_\infty\end{pmatrix}\middle|\ \text{有 } n\in\mathbb{N}\text{ 使 } w\in\mathrm{GL}_n(R)\right\}$ 使 $upu^{-1}=q$(大相似),其中 p,q 视为 $R^{\infty\times\infty}$ 中元素。

证 (1) $\Rightarrow$ (2):由设知 $P=pR^m$,$Q=qR^n$,$R^m=pR^m\oplus(1-p)R^m$,$R^n=qR^n\oplus(1-q)R^n$。将同构 $pR^m\overset{\alpha}{\simeq}qR^n$ 开拓为同态 $(\alpha,0):R^m\to R^n$,将 α^{-1} 开拓为同态 $(\alpha^{-1},0):R^n\to R^m$(注意直和项上的同态一定可以开拓),则 $(\alpha,0)$ 相当于左乘 $y\in R^{m\times n}$,$(\alpha^{-1},0)$ 相当于左乘 $x\in R^{n\times m}$,且 $p=xy$,$q=yx$,对

应到 $R^{\infty\times\infty}$ 即得(2)。

(2) ⇒(3)：对已知的 $p=xy, q=yx$，取 $a=pxq, b=qyp$，则有

$$ab=(pxq)(qyp)=pxqyp=pxyxyp=p^4=p$$

同理有

$$ba=(qyp)(pxq)=q$$

又由 a、b 之取法知 $a=pa=aq$，$b=qb=bp$，于是

$$\begin{pmatrix}1-p & a\\ b & 1-q\end{pmatrix}^2=I_{m+n} \qquad (m+n\text{ 阶单位方阵})$$

记

$$u_1=\begin{bmatrix}1-p & a & \\ b & 1-q & \\ & & I_\infty\end{bmatrix}$$

则 $u_1^2=I_\infty$，因此 $u_1=u_1^{-1}$ 且

$$u_1\begin{pmatrix}p & \\ & 0_\infty\end{pmatrix}u_1^{-1}=u_1\begin{bmatrix}0 & a & \\ 0 & 0 & \\ & & 0_\infty\end{bmatrix}=\begin{bmatrix}0 & & \\ & q & \\ & & 0_\infty\end{bmatrix}$$

右端经对应置换矩阵 $T\in R^{\infty\times\infty}$ 给出的相似变换(行对调与相应的列对调)即得 $\begin{pmatrix}q & \\ & 0_\infty\end{pmatrix}$。故取 $u=Tu_1$ 即得 $upu^{-1}=q$。

(3) ⇒(1)：由 $upu^{-1}=q$ 知 u 对应着同构且 $up=qu$ 故有 $p=\mathrm{Im}p\simeq \mathrm{Im}q=Q$。 □

注① 在引理 2.1 的条件下，不妨设 $m>n$，于是 $q^2=q\in R^{n\times n}$ 可看作是 $\begin{bmatrix}q & \\ & 0_{m-n}\end{bmatrix}$，因此 p、q 都是 $R^{m\times m}$ 中的幂等阵。改此引理中的(2)，(3)各为

(2)′：有 $x,y\in R^{m\times m}$ 使 $p=xy, q=yx$

(3)′：有 $u\in \mathrm{GL}_m(R)$ 使 $upu^{-1}=q$

[Berrick 2000]证明了：(3)′ $\underset{\not\Leftarrow}{\Rightarrow}$ (1)，[Blackadar, 1986]证明了：(3)′ $\underset{\not\Leftarrow}{\Rightarrow}$ (2)′ (事实上(3)′⇒(1)与(2)′都容易证出的，(1) $\not\Rightarrow$ (3)′(用§1 的例 1)也可证明。建议读者一试。

由此可看出，将矩阵通过上面的方法“变大”的优越性。

现在可来证明如下结果：

命题 2.1 对任意环 R，

(1) 若 $p^2=p, q^2=q\in R^{\infty\times\infty}$ 满足引理 2.1 中的(2)(或(3))，记为 $p\sim$

q,则"～"为等价关系;

(2) 记$\langle p\rangle$为 $p^2=p\in R^{\infty\times\infty}$ 所在的关于"～"的等价类,规定

$$\langle p\rangle+\langle q\rangle=\langle\begin{pmatrix}p&&\\&q&\\&&0_\infty\end{pmatrix}\rangle=\langle p\oplus q\rangle$$

则 $\mathrm{Idem}(R)=\{\langle p\rangle\mid p^2=p\in R^{\infty\times\infty}\}$为交换半群(且是幺半群);

(3) $\mathrm{Idem}(R)\simeq\mathrm{Proj}(R)$(半群同构)。

证 (1) 由引理 2.1,注意引理 2.1 之(1)中的同构显然为等价关系,即知"～"为等价关系。

(2) 容易看出这里$\langle p\rangle+\langle q\rangle$与等价类代表元选取无关即得(2)。

(3) 由本节开头 $P\in \mathrm{f.g.P}_R\mathfrak{M}$ 与 $p=p^2\in R^{\infty\times\infty}$ 一一对应,用引理 2.1 即得。 □

由§1 中 K_0 群的第一种定义:$\mathrm{K}_0(R)\simeq G(\mathrm{Proj}(R))$用命题 2.1(3)即得下述的:

定理 2.1 $\mathrm{K}_0(R)\simeq G(\mathrm{Idem}(R))$

这就给出了 K_0 群的第三种定义法(即以 $G(\mathrm{Idem}(R))$作为 R 的 K_0 群)——用幂等阵的定义法。

于是我们有了 K_0 群的三种等价的定义:

第一种定义 $\overset{\text{定理 1.1}}{=\!=\!=}$ 第二种定义
(用半群完备化)　　(对自由群加关系)
‖ 定理 2.1
第三种定义
(用幂等阵)

第三种定义法有独特的优点,比如注意到 $R^{\infty\times\infty}=(R^{n\times n})^{\infty\times\infty}$(注意 $R^{\infty\times\infty}$ 元素左上角幂等阵阶数 m 小于 n 或 $m=kn+r,k>0,0<r<n$ 时可通过右下角补 0_{n-m} 或 0_{n-r} 成为 n 阶幂等阵($R^{n\times n}$上 1×1 幂等阵或 $R^{n\times n}$上的$(k+1)\times(k+1)$幂等阵)。由此立得(用其它方法来证十分复杂的)下述结果,它事实上是 K_0 群的一种"弱"Morita 不变性,也常被称为 K_0 群的 Morita 不变性(环 R,S 是 Morita 等价的是指${}_R\mathfrak{M}$与${}_S\mathfrak{M}$(或 $\mathfrak{M}_R$ 与$\mathfrak{M}_S$)为等价范畴,常记为 $R\overset{M}{\approx}S$,可以证明 $R\overset{M}{\approx}R^{n\times n}$, $\forall n\geqslant1$。但 $R\overset{M}{\approx}S$ 推不出有 $n\geqslant1$ 使 $S\simeq R^{n\times n}$)。

定理 2.2 对任意环 R,$\mathrm{K}_0(R)\simeq\mathrm{K}_0(R^{n\times n})$, $\forall n\geqslant1$(K_0 群的弱 Morita 不变性)。

事实上，在 $R \overset{M}{\approx} S$ 时也可证 $K_0(R) \simeq K_0(S)$（见[McConnell，1988]）。

由 K_0 群的第三种定义又可立即看出下述结果：

命题 2.2 对任意环 R，用 f. g. $P_R\mathfrak{M}$，f. g. $P\mathfrak{M}_R$（有限生成投射右 R-模范畴）定义的 $K_0(R)$ 是一致的（同构的）。

1966 年 A. Steger 在[Steger，1966]中对任意的交换环 R 与 $n \geqslant 1$，证明了幂等阵具有一个有用的性质：设 $E^2 = E \in R^{n \times n}$，则有 $P, Q \in GL_n(R)$ 使 PEQ 为对角阵 $\Leftrightarrow$ E 相似于对角阵（当然对角阵的对角元都是 R 的幂等元）。

如果对交换环 R，及任意的 $n \geqslant 2$，$R^{n \times n}$ 中的幂等阵都可（用相似变换）对角化，则称 R 为 **PT 环**（projective trivial ring），记为 $R \in PT$，可证：当 $I \subset J(R)$，$R/I \in PT$ 时，必有 $R \in PT$，且 PT 环对 $\oplus$ 封闭，见[McDonald，1984]。对 R 的素根 $\mathrm{rad}(R) \equiv \bigcap\limits_{\substack{p \lhd R \\ \text{prime}}} P$。若 $I \subset \mathrm{rad}(R)$，则更进一步地有 $R \in PT \Leftrightarrow P/I \in PT$。用第三种定义可立知：若 $R \in PT$ 为连通环（只有 0，1 为幂等元的环，也称为不可分解环），则 $K_0(R) \simeq \mathbb{Z}$。事实上，我们可证更强的下述结果：

命题 2.3 设 $R \in PT$ 为连通环，则 R 为 PF 环（即 $K_0(R) \simeq \mathbb{Z}$，且 $R \in SFF = UCP$）。

证 $\forall P \in$ f. g. $P_R\mathfrak{M}$，由前知 $P = \mathrm{Im}p$，可设 $p^2 = p \in R^{n \times n}$，$upu^{-1} = \mathrm{diag}(e_1, \cdots, e_n)$，则

$$P = \mathrm{Im}p \simeq \mathrm{Im}(upu^{-1}) \simeq Re_1 \oplus \cdots \oplus Re_n$$

不失一般地设 $0 \neq e_i^2 = e_i \in R, i = 1, \cdots, t$。$e_j = 0, j = t+1, \cdots, n$。由 R 连通知 $e_1 = \cdots = e_t = 1$。于是 $P \simeq R^t$，即 $P \in$ f. g. $\mathrm{Free}_R\mathfrak{M}$。由 P 的任意性即知 $R \in PF$。 □

注意在交换环范畴中，零维环（对 Krull 维数，比如 Artin 环即为零维环），整体维数为 0 的环（即 Artin 半单环），弱维数为 0 的环（即 von Neumann 正则环），半局部环（当然包括局部环），PID，Bezout 环等都是 PT 环（见[McDonall，1984]，同时容易看出 $PF \subset PT \subset SFF(= UCP)$，对整环，$PT = SFF$（见[McDonald，1984]）。

在 §4 中我们将用[佟文廷，1994]中的结果将命题 2.3 改进为：对交换环 R，$R \in PT$ 且 R 连通 $\Leftrightarrow R \in PF$。

下面来研究 K_0 的函子性，不熟悉函子的读者可参看[佟文廷，1998]的第一章。

设 R, S 为环，$f: R \to S$ 为环同态（本书的环同态均保持单位元）。由此

知 $S\in {}_S\mathfrak{M}_R$(在 f 作用的意义下规定 $sxr=sxf(r)$,$\forall r\in R,s,x\in S$)。记

$$S\underset{f}{\otimes}P=S\underset{R}{\otimes}P,\qquad \forall P\in {}_R\mathfrak{M}$$

由 $S\underset{f}{\otimes}R\simeq S$ 知,当 $P\oplus Q\simeq R^n$ 时有左 S-模同构。

$$\begin{aligned}&(S\underset{f}{\otimes}P)\oplus(S\underset{f}{\otimes}Q)\\ &\simeq S\underset{f}{\otimes}(P\oplus Q)\simeq S\underset{f}{\otimes}R^n\simeq(S\underset{f}{\otimes}R)^n\simeq S^n\end{aligned}$$

因此,$S\underset{f}{\otimes}P\in \text{f. g. P}_S\mathfrak{M}$,$\forall P\in \text{f. g. P}_R\mathfrak{M}$,于是可定义

$$\begin{aligned}f_*\equiv \mathrm{K}_0(f):\mathrm{K}_0(R)&\longrightarrow \mathrm{K}_0(S)\\ [P]&\longmapsto [S\underset{f}{\otimes}P]\end{aligned}$$

注① 上述 S 的 R-模结构是由 f 给出的!当 $f:R\longrightarrow R$ 为环的满同态且 $\mathrm{Ker}f=I$(R 的理想)时,后一个环 R(事实上即 R/I)作为前一个环 R 上的模应看作 R/I(考虑模乘法)。因此 $\mathrm{K}_0(f)([P])=[R/I\underset{f}{\otimes}P]\neq[R\underset{R}{\otimes}P]$,而不能简单地写为 $\mathrm{K}_0(f)([P])=[P]$,$\forall P\in \text{f. g. P}_R\mathfrak{M}$。由此可看出记号$\underset{f}{\otimes}$比$\underset{R}{\otimes}$的含义更明确。

在上述记号下,我们有:

命题 2.4 设 $f:R\longrightarrow S$ 为环同态,则

(1) $f_*\equiv\mathrm{K}_0(f):\mathrm{K}_0(R)\longrightarrow\mathrm{K}_0(S)$为 Abel 群同态;

(2) 当 R,S 为交换环时,$f_*\equiv\mathrm{K}_0(f)$又是环同态。

证 (1) 任取 $P_1,P_2\in \text{f. g. P}_R\mathfrak{M}$,则

$$\begin{aligned}f_*([P_1]+[P_2])&=f_*([P_1\oplus P_2])=[S\underset{f}{\otimes}(P_1\oplus P_2)]\\ &=[(S\underset{f}{\otimes}P_1)\oplus(S\underset{f}{\otimes}P_2)]\\ &=[S\underset{f}{\otimes}P_1]+[S\underset{f}{\otimes}P_2]=f_*([P_1])+f_*([P_2])\end{aligned}$$

因此 f_* 为群同态。

(2) 当 R,S 为交换环时 $\mathrm{K}_0(R)$,$\mathrm{K}_0(S)$都是交换环,且对任意的 $P_1,P_2\in \text{f. g. P}_R\mathfrak{M}$ 有

$$\begin{aligned}(S\underset{f}{\otimes}P_1)\underset{S}{\otimes}(S\underset{f}{\otimes}P_2)&\simeq(P_1\underset{R}{\otimes}S)\underset{S}{\otimes}(S\underset{R}{\otimes}P_2)\\ &\simeq P_1\underset{R}{\otimes}(S\underset{R}{\otimes}P_2)\simeq S\underset{R}{\otimes}(P_1\underset{R}{\otimes}P_2)\\ &\simeq S\underset{f}{\otimes}(P_1\underset{R}{\otimes}P_2)\end{aligned}$$

由此知,f_* 保持乘法对应。又 $S\underset{f}{\otimes}R\simeq S$,因此 f_* 保持单位元对应。故 f_* 为环同态。 □

注意到上述命题中 $K_0(f)([R])=[S]$，由命题 1.3 立得下述已知结果的简单证明：

推论 2.1 设有环同态 $f:R\longrightarrow S$，且 $S\in \mathrm{IBN}$，则 $R\in \mathrm{IBN}$。

记 Ring、AG（即 $_{\mathbb{Z}}\mathfrak{M}$），CRing 各为环范畴，Abel 群范畴与交换环范畴，我们有

定理 2.3 K_0：Ring $\longrightarrow$ AG 是共变函子；

K_0：CRing $\longrightarrow$ CRing 也是共变函子。

证 设 $f:R\longrightarrow S, g:S\longrightarrow T$ 都是环同态，则

$$T\underset{g}{\otimes}(S\underset{f}{\otimes}P)\simeq(T\underset{g}{\otimes}S)\underset{f}{\otimes}P\simeq T\underset{gf}{\otimes}P,\qquad \forall P\in \text{f. g. }P_R\mathfrak{M},$$

因此

$$K_0(g)K_0(f)=K_0(gf)$$

又对恒等同态 $I_R:R\to R$，显然有

$$K_0(I_R)=I_{K_0(R)}:K_0(R)\to K_0(R)$$

故 K_0：Ring$\to$AG 为共变函子。

后一结论是显见的。 □

利用 K_0 的函子性可得到一些有趣的应用，先来证明如下命题：

命题 2.5 设有环同态 $f:R\to S$ 与 $g:S\to R$ 使 $gf=I_R$，则

(1) $K_0(f)$ 为单同态，因此在同构意义下，$K_0(R)$ 为 $K_0(S)$ 的子群（当 R,S 都为交换环时为子环）。记为 $K_0(R)\lesssim K_0(S)$；

(2) $K_0(g)$ 为满同态，因此 $K_0(R)$ 为 $K_0(S)$ 的商群（R,S 为交换环时为商环）；

(3) 有 Abel 群同构

$$K_0(S)\simeq K_0(R)\oplus \mathrm{Ker}K_0(g)=\mathrm{Im}K_0(g)\oplus \mathrm{Ker}K_0(g);$$

(4) 若 $S\in \mathrm{PSF}$，则 $R\in \mathrm{PSF}$。

证 由 K_0 的函子性知

$$K_0(g)K_0(f)=K_0(gf)=K_0(I_R)=I_{K_0(R)}$$

由此即得(1)、(2)。而(1) ⇒(4)是显见的（注意 $S\in \mathrm{PSF}\Leftrightarrow K_0(S)=\mathbb{Z}[S]$ 且 $K_0f([R])=[S]$，再由 $K_0(f)$ 单即知 $K_0(R)=\mathbb{Z}[R]$）。

再由 AG 中正合列

$$0\to \mathrm{Ker}K_0(g)\to K_0(S)\xrightarrow{K_0(g)}\mathrm{Im}K_0(g)\to 0$$

$$\| \; K_0(g) \text{ 满}$$

$$K_0(R)$$

的可裂性（由 $K_0(g)K_0(f)=I_{K_0(R)}$ 知）即得(3)。 □

由此命题可立得如下的有用推论：

推论 2.2 设 R 为任意环，$S=R[x_1,\cdots,x_n]$，$f:\begin{array}{c}R\rightarrowtail S\\ r\mapsto r\end{array}$ 为标准单同态，$g:S\twoheadrightarrow R$ 使 $g(h(x_1,\cdots,x_n))=h(0,\cdots,0)$（即对 n 元多项式取常数项），则 $gf=I_R$. 因此 $K_0(f)$ 为单同态，$K_0(g)$ 为满同态且

$$K_0(R[x_1,\cdots,x_n])\simeq K_0(R)\oplus \mathrm{Ker}K_0(g)$$

推论 2.3 设 R 为任意环，G 为（乘法）群，$S=RG$（R 上关于 G 的群环），则 $f:\begin{array}{c}R\rightarrowtail S\\ r\mapsto re_G\end{array}$，$g:\begin{array}{c}S\twoheadrightarrow R\\ \Sigma r_jg_j\mapsto\Sigma r_j\end{array}$ 为环同态，且 $gf=I_R$。因此 $K_0(f)$ 为单同态，$K_0(g)$ 为满同态，同时

$$K_0(RG)\simeq K_0(R)\oplus \mathrm{Ker}K_0(g)$$

注② 命题 2.5、推论 2.2、推论 2.3 中将 K_0 换成其他共变函子 F: Ring→AbG 时也真（同法证）。因此这三个结果对一切 K-群（如本书后面的 K_1 群 K_2 群）都真。

注③ 设 R 为左 Noether 环且任一有限生成左 R-模都有有限的投射维数（左整体维数 $\mathrm{lg}D(R)$ 可以是∞）则称 R 为**左正则环**(left regular ring)，J. P. Serre 给出一种处理分次环的办法证明了下述的 Grothendieck 定理（见[Bass, 1968]）：设 R 为左正则环，T 为自由交换幺半群或自由 Abel 群，则 $K_0(R)$ 与 $K_0(R[T])$ 同构。因此 $K_0(R[x_1,\cdots,x_n])\simeq K_0(R)$。事实上，他证明了更一般的结果：设 $R=\bigoplus_{n\geq 0}R_n$ 为分次左正则环，则包含映射（同态）$i:R_0\to R$ 诱导出一个群同构 $K_0(i):K_0(R_0)\to K_0(R)$。此外对正则环 R，还可证明 $K_0(R)\simeq K_0(\triangle(R))\simeq K_0(\mathcal{D}(R))$，其中 $\triangle(R)$ 为 R 上的导子环，而 $\mathcal{D}(R)$ 为 R 上的微分算子环（见[McConnell, 1988]）。

注意在有单位元环范畴 Ring 中通常的环直积（也称直和）$\bigoplus_{j=1}^{n}R_j$ 已不是范畴意义下的直和。这是因为

$$\begin{array}{ccc}R_j & \longrightarrow & \bigoplus_{j=1}^{n}R_j\\ 1_{R_j} & \longmapsto & (0,\cdots,0,1_{R_j},0,\cdots,0)\end{array}$$

已不保持单位元的对应（$\bigoplus_{j=1}^{n}R_j$ 的单位元为 $(1_{R_1},\cdots,1_{R_n})$！），从而不是通常意义下的环同态。因此无法直接应用命题 2.5。虽然可用模论的方法（较繁地）证出下述结果（见[Silvester, 1981]）。但用 K_0 群的第三种定义可给出非常简单的下述证法。

命题 2.6 设环 $R=\bigoplus\limits_{j=1}^{n}R_j$，则 $K_0(R)\simeq\bigoplus\limits_{j=1}^{n}K_0(R_j)$，即 K_0 函子与$\oplus$可以交换。

证 由归纳法原理知，只需证 $n=2$ 的情况。可设 $R=R_1\oplus R_2$ 注意到

$$\mathrm{Idem}(R)=\mathrm{Idem}(R_1)\times\mathrm{Idem}(R_2)$$

$$\mathrm{GL}(R)=\mathrm{GL}(R_1)\times\mathrm{GL}(R_2)$$

用定理 2.1 即得证。 □

这里我们又一次看到 K_0 群的第三种定义的优越性。

由命题 2.6 可以方便地求出一些环的 K_0 群。

例 1 设 $R=\mathbb{Z}/p_1\cdots p_n\mathbb{Z}$，$p_1,\cdots,p_n$ 为 n 个不同的素数，由

$$\mathbb{Z}/p_1\cdots p_n\mathbb{Z}\simeq\mathbb{Z}/p_1\mathbb{Z}\oplus\cdots\oplus\mathbb{Z}/p_n\mathbb{Z}$$

为 n 个域的直和知有 Abel 群同构（也是环同构）

$$K_0(\mathbb{Z}/p_1\cdots p_n\mathbb{Z})\simeq\mathbb{Z}^n$$

更一般地，注意$\mathbb{Z}/p_i^{a_i}\mathbb{Z}$ 为局部环（$a_i\geqslant1$），也有 Abel 群（环）同构

$$K_0(\mathbb{Z}/p_1^{a_1}\cdots p_n^{a_n}\mathbb{Z})\simeq\mathbb{Z}^n$$

下面再来简单地介绍一下，如何从（有单位元）环的 K_0 群去定义无单位元环的 K_0 群。

设 I 为环（未必有单位元，如环的理想）记为 $I\in\mathrm{Rng}$，如众所周知，在 $I_+\equiv I\oplus\mathbb{Z}\in\mathrm{AG}$ 中定义乘法（记号 I_+ 来自拓扑学、拓扑空间 X 上加一个基点后，常记为 X_+）：

$$(x,n)(y,m)=(xy+mx+ny,mn),\ \forall x,y\in I,m,n\in\mathbb{Z}$$

则使 $I_+\equiv I\oplus\mathbb{Z}\in\mathrm{Ring}$，其单位元为 $1_{I_+}=(0,1)$。

容易验证Rng 中的同态 $\beta:I\to I'$诱导出Ring 中的（保单位元）同态

$$\beta_+:I_+\longrightarrow I'_+,\quad (x,n)\longmapsto(\beta(x),n)$$

因此这里的下标“+”事实上是共变函子$+:\mathrm{Rng}\longrightarrow\mathrm{Ring}$。当 $I\in\mathrm{Ring}$（即 1_I 存在）时，定义

$$\alpha:I_+\longrightarrow I\oplus\mathbb{Z}\text{（有单位元环之直积）},$$

$$(x,n)\longmapsto(x+n\cdot 1_I,n)$$

则可看出 α 为一一对应且使$\alpha(0,1)=(1_I,1)$，同时

$$\begin{aligned}\alpha((x,n)(y,m))&=\alpha((xy+mx+ny,mn))\\&=(xy+mx+ny+mn\cdot 1_I,mn)\\&=(x+n\cdot 1_I,n)(y+m\cdot 1_I,m)\\&=\alpha((x,n))\alpha((y,m))\end{aligned}$$

故得：

引理 2.2　设 $I\in$ Rng，则上述的 $\alpha: I_+\to I\oplus\mathbb{Z}$ 为(保单位元的)环同构。

显然有加法 Abel 群正合列(不要求 I 有单位元)

$$0\longrightarrow I\xrightarrow{\ i\ } I_+\xrightarrow{\ g\ }\mathbb{Z}\longrightarrow 0,$$

这里，$i(x)=(x,0)$，$g(x,n)=n$，$\forall x\in I, n\in\mathbb{Z}$，其中的 g 也是 Ring 中的环同态(i 不是!)。于是有群同态 $g_*=\mathrm{K}_0(g):\mathrm{K}_0(I_+)\longrightarrow\mathrm{K}_0(\mathbb{Z})\simeq\mathbb{Z}$。定义 $\mathrm{K}_0(I)=\mathrm{Ker}g_*$ 即得 $I\in$ Rng 的 K_0 群。

现来证明：

命题 2.7　当 $I\in$ Ring 时这一定义与前面的定义是一致的。

证　当 $I\in$ Ring 时，则对上述的 g 有 Ring 中的环同态 $f:\ \mathbb{Z}\longrightarrow I_+,\ n\longmapsto(0,n)$ 使 $gf=I_{\mathbb{Z}}$。因此由命题 2.5(3)之证知有可裂的 Abel 群正合列

$$0\longrightarrow \mathrm{Ker}g_*\longrightarrow \mathrm{K}_0(I_+)\xrightarrow{\ g_*\ }\mathrm{K}_0(\mathbb{Z})\longrightarrow 0$$

故有 $\mathrm{K}_0(I_+)\simeq\mathrm{Ker}g_*\oplus\mathrm{K}_0(\mathbb{Z})\simeq\mathrm{Ker}g_*\oplus\mathbb{Z}$。

再由引理 2.2 知有 Ring 的环同构 $I_+\overset{\alpha}{\simeq}I\oplus\mathbb{Z}$，于是由命题 2.6 知

$$\mathrm{K}_0(I_+)\simeq\mathrm{K}_0(I)\oplus\mathrm{K}_0(\mathbb{Z})\simeq\mathrm{K}_0(I)\oplus\mathbb{Z}$$

由此知

$$\mathrm{Ker}g_*\oplus\mathbb{Z}\simeq\mathrm{K}_0(I)\oplus\mathbb{Z}$$

注意 $\mathbb{Z}$ 是直和可消的(在 $\mathbb{Z}\mathfrak{M}=$ AG 中)(见[Cohn，1956]或[Walker，1956])，故 $\mathrm{Ker}g_*\simeq\mathrm{K}_0(I)$，即，这一定义与前面的 K_0 群定义对 Ring 是一致的。　□

注④　注意由 Ring 到 Rng 放松了对同态保持单元对应的要求。比如 $R\in$ Ring，$n>1$，在 Ring 中只有一种同态 $f:R\to R^{n\times n}$，即 $f(r)=rI_n$ 给出的环同态，而且不存在从 $R^{n\times n}$ 到 R 的任何同态。但在 Rng 中只要定义 $f(r)=\begin{pmatrix} r & 0 & \cdots & 0\\ 0 & & & \\ \cdots & & 0 & \\ 0 & & & \end{pmatrix}$，$\forall r\in R$ 就能给出 R 到 $R^{n\times n}$ 的同态，而且零同态就是 $R^{n\times n}$ 到 R 的同态。对于 Rng，$\oplus$ 则是范畴意义下的直积。K_0：Rng$\to$AG 为函子，因此由命题 2.7 可立得 $\mathrm{K}_0(R_i)$ 都是 $\mathrm{K}_0(\oplus R_i)$ 的直和项。

利用本节的定理 2.2 我们可给出例子说明上节的命题 1.7($R\in$ IBN 且

$R\in \mathrm{PSF}\Leftrightarrow \mathrm{K}_0(R)\overset{f}{\simeq}\mathbb{Z}$ 且使 $f([R])=1$)中条件"$f([R])=1$"是必不可少的,同时也说明在 $\mathrm{K}_0(R)\simeq\mathbb{Z}$ 的情况下$[R]$未必为 $\mathrm{K}_0(R)$的生成元。

例 2 设 F 为域,$R=F^{n\times n}$,$n>1$。

由定理 2.2 知 $\mathrm{K}_0(R)\simeq\mathbb{Z}$,但 $F^n\equiv F^{n\times 1}\in {}_R\mathfrak{M}$ 且 $R\simeq \underbrace{F^n\oplus\cdots\oplus F^n}$ $\in {}_R\mathfrak{M}$,因此 $F^n\in \mathrm{f.g.\,P}_R\mathfrak{M}$ 且$[R]=n[F^n]$。由此知$[F^n]\notin\mathbb{Z}[R]$,因此$[R]$不是 $\mathrm{K}_0(R)$的生成元且 $F^n\notin \mathrm{SF}_R\mathfrak{M}$(命题 1.6)。由此知 $R\notin \mathrm{PSF}$。注意到环 $S\in\mathrm{IBN}\Leftrightarrow\forall\, m\neq n$,不存在 $A\in S^{m\times n}$,$B\in S^{n\times m}$使 $AB=I_m$,$BA=I_n$(容易直接用基底的 S-线性变换证此结果,也可见[Cohn,1979]),立知这里的 R(由于 $F\in\mathrm{IBN}$)为 IBN 环。因此,即使对 IBN 环,$R\in\mathrm{PSF}$ 与 $\mathrm{K}_0(R)\simeq\mathbb{Z}$ 一般地也并不等价。

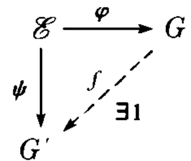
由此例容易看出与 Morita 等价相关的一个结果。

命题 2.8 设 $S=R^{n\times n}$为任意环R 上的 $n\times n$ 矩阵环,则在 $\mathrm{K}_0(S)$的生成系$\{[P]\mid P\in \mathrm{f.g.\,P}_S\mathfrak{M}\}$中 $n\mid[S]$,即有 $P\in \mathrm{f.g.\,P}_S\mathfrak{M}$ 使 $n[P]=[S]$。

这条命题是用 K_0 群判定一个环不是任何环上矩阵环的有效方法之一(见[McConnell,1988])。

在本节中我们已站在范畴的高度看到 K_0 的函子性。现在我们顺便再看看:为什么 $\mathrm{K}_0(R)$的几种定义中都立足于 $\mathrm{f.g.\,P}_R\mathfrak{M}$ 而不用 $P_R\mathfrak{M}$(投射 R-模范畴)?如果立足于 $\mathrm{f.g.}\,{}_R\mathfrak{M}$(有限生成 R-模范畴)如何?我们先粗略地介绍一下 K_0 群的范畴定义法(更精确更详细地介绍将放在§15)。

1. 设 $\mathscr{C}$ 为带积范畴(即 $\mathscr{C}$ 有零对象且有共变函子$\perp:\mathscr{C}\times\mathscr{C}\to\mathscr{C}$ 使 $A\simeq A\perp 0\simeq 0\perp A$,$A\perp B\simeq B\perp A$,$A\perp(B\perp C)\simeq(A\perp B)\perp C$,$\forall A,B,C\in\mathscr{C}$,比如 $\mathscr{C}=\mathrm{f.g.\,P}_R\mathfrak{M}$,$\mathrm{P}_R\mathfrak{M}$,${}_R\mathfrak{M}$,$\mathrm{f.g.}\,{}_R\mathfrak{M}$,…对于$\oplus$都是带积范畴)。令 $G\in\mathcal{A}\mathrm{G}$,$\varphi$:$\mathscr{C}\to G$ 满足 $A\simeq A'$时 $\varphi(A)=\varphi(A')$且 $\varphi(A\perp B)=\varphi(A)+\varphi(B)$(此时称 φ 为保积映射)。若(G,φ)满足如下泛性质:对任意的 $G'\in\mathcal{A}\mathrm{G}$ 与保积映射 ψ:$\mathscr{C}\to G'$有惟一的群同态 $f:G\to G'$使右图为交换图,则称 G 为 $\mathscr{C}$ 的 K_0 群,并记它为 $\mathrm{K}_0(\mathscr{C})$。



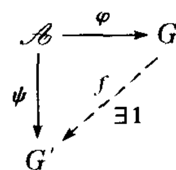
容易看出在同构意义下(若有保积映射 φ:$\mathscr{C}\to G$)$\mathrm{K}_0(\mathscr{C})$存在惟一,且

$$\mathrm{K}_0(\mathrm{f.g.\,P}_R\mathfrak{M},\oplus)=\mathrm{K}_0(R)$$

2. 设 $\mathscr{A}$ 为正合范畴(即 $\mathscr{A}$ 有零对象且 $\forall A,B\in\mathscr{A}$,有 $\xi(A,B)\in\mathscr{A}$ 使

$$0\longrightarrow A\longrightarrow \xi(A,B)\longrightarrow B\longrightarrow 0$$

为 $\mathscr{A}$ 中正合列)。令 $G\in\mathcal{A}\mathrm{G}$,$\varphi$:$\mathscr{A}\longrightarrow G$ 满足 $A\simeq A'\in\mathscr{A}$ 时 $\varphi(A)=\varphi(A')$



且 $\varphi(A)+\varphi(B)=\varphi(\xi(A,B))$,同时$(G,\varphi)$满足如下泛性质:对任意 $G'\in \mathscr{AG}$ 与具有上述性质的 $\psi:\mathscr{A}\longrightarrow G'$ 有惟一的群同态 f 使右图为交换图。此时称 G 为 $\mathscr{A}$ 的 K_0 群,记作 $K_0(\mathscr{A})$,显然当(G,φ)存在时 $K_0(\mathscr{A})$是存在且惟一的(同构意义下)。

对 f. g. $P_R\mathfrak{M}$ 也可由正合范畴的办法定义 $K_0(R)=K_0(\text{f. g. }P_R\mathfrak{M})$(取 $\xi(P,Q)=P\oplus Q$),对 f. g. $_R\mathfrak{M}$ 也可用带积范畴与正合范畴两种办法定义 $K_0(R)$(所得结果当然是一致的)。经常记 $K_0(\text{f. g. }_R\mathfrak{M})$ 为 $G(R)$(见[Bass,1968]与本书§16),容易证明下述命题。

命题 2.9 设 $\mathscr{C}$ 为带积范畴且对无穷(可数)积是封闭的(比如 $P_R\mathfrak{M}$),则 $K_0(\mathscr{C})=0$ 为平凡群,因此 $K_0(P_R\mathfrak{M})=0$。

证 $\forall A\in\mathscr{C}$,取$\perp A=B$,则 $A\perp B\simeq B$。于是,注意到 G 实质上是 $\mathscr{C}$ 中对象同构类的半群之群完备化,记 $A,B\in\mathscr{C}$ 对应 $K_0(\mathscr{C})$的元素分别为$[A]$、$[B]$,有

$$[A]+[B]=[B]$$

因此$[A]=0$,故 $K_0(\mathscr{C})=0$。 □

由此命题知若以 $P_R\mathfrak{M}$ 代替 f. g. $P_R\mathfrak{M}$ 或以$_R\mathfrak{M}$ 代替 f. g. $_R\mathfrak{M}$ 都只能得到平凡的 K_0 群。

§3 半局部环的 K_0 群与环的约化群

定义 3.1 设 R 为环(未必为交换环),若 $R/J(R)$为左(右)Artin 环,其中 $J(R)$为 R 的 Jacobson 根,则称 R 为**半局部环**(semilocal ring)。

显然 R 为半局部环$\Leftrightarrow R/J(R)$为半单 Artin 环(不分左、右)。

半局部环是概括广的一大环类,由定义立知:域、除环当然是半局部环,局部环(使 $R/J(R)$为除环的环)也是半局部环。可以证明 R 为局部环$\Leftrightarrow R$ 有惟一的左(右)极大理想$\Rightarrow R$ 有惟一极大理想(在 $R\in\mathscr{C}$Ring 时,这里的“$\Rightarrow$”可加强为“$\Leftrightarrow$”,但 $R\notin\mathscr{C}$Ring 时不行,比如 $\mathbb{Z}^{n\times n}$有惟一极大理想 0,但 $\mathbb{Z}^{n\times n}$非局部环)。另外,由于左(右)Artin 环的同态象仍为左(右)Artin 环,左(右)Artin 环(比如有限环,Frobenius 环,QF 环都是 Artin 环)当然也是半局部环。还有两类环:完全环(perfect ring)与半完全环,也都是半局部环。这里说的左(右)完全环是满足下述等价条件之一的环:(1) $R/J(R)$为

半单 Artin 环且 $J(R)$ 为左(右)T 幂零的(这里的 T 表示 transfinite,即 $\forall a_1,a_2,\cdots,\in J(R)$ 必有 n 使 $a_1a_2\cdots a_n=0(a_n\cdots a_2a_1=0)$);(2) 右(左)主理想满足 DCC(降链条件);(3) 平坦左(右)R-模都是左(右)R-投射模;(4) 任一左(右)R-模 M 都有投射盖(projective cover),即有 $P\in \mathrm{P}_R\mathfrak{M}(\mathrm{P}\mathfrak{M}_R)$ 与满同态 $\varepsilon:P\to M$ 具有如下泛性质:对任意的 $Q\in \mathrm{P}_R\mathfrak{M}(\mathrm{P}\mathfrak{M}_R)$ 与满同态 $\psi:Q\to M$ 必有满同态 $\varphi:Q\to P$ 使 $\psi=\varepsilon\varphi$;(5) R 的每一商环都满足上述等价条件之一。对这种环,需注意左(右)完全环未必是右(左)完全环。Jacobson 根是幂零的局部环称为完全准素(completely primary)环,其上的矩阵环称为准素环,Jacobson 根是幂零的半局部环称为半准素环。显然,准素环为半准素环,半准素环为左(右)完全环。而半完全环(不分左右,左半完全环即右半完全环)是指满足下述等价条件之一的环:(1) 任意的 $M\in \mathrm{f.g.}\,{}_R\mathfrak{M}$ 都有投射盖;(2) $R/J(R)$ 为 Artin 半单环且幂等元 $\mathrm{mod}J(R)$ 可以提升(即 $\forall \bar{e}^2=\bar{e}\in R/J(R)$,必有 $e=e^2\in R$ 使 $e+J(R)=\bar{e}$);(3) 单左 R-模都有投射盖;(4) 一切商环都满足上述等价条件之一。

注① 设环 R 满足 $R^2=R$(Ring 中的环当然满足此条件,但 Ring 中满足 $R^2=R$ 的环 R 未必有单位元,当然也未必为交换环),对 R 的任一极大理想 M,由 $A,B\not\subset M$,$A,B\lhd R$ 易推出 $AB\not\subset M$(注意 $A+M=R=B+M$),因此 M 必为 R 的素理想。由此可证(有单位元的)Artin 环的极大理想个数必有限,因此,半局部环的极大理想(都含 Jacobson 根!)个数也必有限。对交换环 R 容易证明:R 为局部环$\Leftrightarrow R$ 的极大理想只有 1 个$\Leftrightarrow R=R^{\cdot}\dot{\cup}J(R)$。其中 $R^{\cdot}$ 为 R 的乘法群,$\dot{\cup}$ 表直并;可证此时 R 为半局部环$\Leftrightarrow R$ 只有有限个极大理想。

为研究半局部环的 K_0 群,先证明一条十分有用的著名引理。为了方便读者更好地理解下文,我们给出它的一般形式。

引理 3.1 (NAK 引理,Nakayama 引理)设 I 为任意环 R 的左理想,则下述四点是等价的:

(1) $I\subseteq J(R)$;

(2) $\forall M\in \mathrm{f.g.}\,{}_R\mathfrak{M}$,若 $L<M$ 使 $M=L+IM$,则 $M=L$;

(3) $\forall M\in \mathrm{f.g.}\,{}_R\mathfrak{M}$,若 $IM=M$,则 $M=0$;

(4) $1+I=\{1+a\mid a\in I\}$ 为 R 的乘法群 $R^{\cdot}$(也常记为 $U(R)$)的子群。

为证引理 3.1,先回顾一下 $M\in {}_R\mathfrak{M}$ 的 Jacobson 根的定义并证明两条引理。

设 $M\in {}_R\mathfrak{M}$,M 的一切极大子模之交称为 M 的 Jacobson 根,记为 $J(M)$

(当 M 无极大子模时常约定 $J(M)=M$。但事实上容易证明:当 M 为有限生成模时(比如 R),M 必有极大子模)。

引理 3.2 $\forall M\in {}_R\mathfrak{M}$,

$$J(M)=\bigcap\{\mathrm{Ker}\gamma \mid \gamma: M\to S \text{ 为模同态}, S \text{ 为左} R\text{-单模}\}。\tag{1}$$

因此 $J(R)M\subseteq J(M)$(事实上对半局部环 R,还可证 $J(R)M=J(M)$,见[Xue,1992])。

证 任取 M' 为 M 的极大子模,则 M/M' 为单模,因此取 $\gamma:M\to M/M'$ 为标准同态知 $M'=\mathrm{Ker}\gamma$。另一方面若 S 为左 R-单模且有非零模同态 $\gamma:M\to S$ 则由 S 的单性知 γ 必为满同态,因此 $S\simeq M/\mathrm{Ker}\gamma$,于是 $\mathrm{Ker}\gamma$ 为 M 的极大子模。由此知 $J(M)=\bigcap\{\mathrm{Ker}\gamma \mid \gamma:M\to S$ 为模同态,S 为左 R 单模$\}$。取上段证明中的 $M=R$,S 为单模,任取 $0\neq x\in S$ 定义 $\beta:R\to S$ 使 $\beta(r)=rx$,$\forall r\in R$。则 $\beta(J(R))=0$,于是 $J(R)S=0$。再任取 $\gamma:M\to S$ 为任意非零同态,则 $\gamma(J(R)M)\subseteq J(R)S=0$,即 $J(R)M\subseteq \mathrm{Ker}\gamma$。于是由 $J(M)$ 的上述表示式(1)知 $J(R)M\subseteq J(M)$。 □

引理 3.3 设 $M\in \mathrm{f.g.}\,{}_R\mathfrak{M}$,$M'$ 为 M 的子模,则 $M'\subseteq J(M)\Leftrightarrow L$ 为 M 的子模且 $M'+L=M$ 时,必有 $L=M$。

证 $\Rightarrow$:设 L 为 M 的真子模,即 $L\subsetneqq M$,注意 $M'\subseteq J(M)$ 即指 M 的极大子模都包含 M',于是必有 M 的极大子模(包含 L 者)包含 $M'+L$,这与 $M'+L=M$ 矛盾,故 $L=M$。

$\Leftarrow$:只需证 M 的极大子模都包含 M'。事实上,任取 N 为 M 的极大子模,若 $M'\not\subset N$,则 $M'+N=M$,于是 $N=M$,这与 N 为极大子模矛盾,从而引理证毕。 □

引理 3.1(NAK 引理)之证:

(1)$\Rightarrow$(2):由引理 3.2 与引理 3.3 即得。

(2)$\Rightarrow$(3):(2)中取 $L=0$ 即得(3)。

(3)$\Rightarrow$(2):用 M/L 代替(3)中的 M 即由(3)得(2)。

(2)$\Rightarrow$(4):令 $x\in I$,$u=1+x$ 即 $1=u-x$ 于是 $R=Ru+IR$ 由(2)(视 Ru 为 L,R 为 M)知 $R=Ru$,因此有 $v\in R$ 使 $vu=1$。但 $u=1+x$,于是 $1=vu=v+vx$,$v=1-vx\in 1+I$,因此 $R=Rv+Rvx\subseteq Rv+I=Rv+IR$。于是注意 $Rv+IR\subseteq R$ 即知 $R=Rv+IR$。由(2)知 $R=Rv$,因此有 $u_1\in R$ 使 $u_1v=1$。由此知 $u_1vu=u$,即 $u_1=u$(注意 $vu=1$),由此知 $u\in R^{\cdot}$。再注意 $1+I$ 对乘法与取逆是封闭的即知(4)成立。

(4)$\Rightarrow$(1):若(1)不成立,则必有 R 的极大左理想 $\mathfrak{m}$ 使 $I\not\subset\mathfrak{m}$,于是 $R=$

$\mathfrak{m}+I$。因此 $1=m+x$，其中 $m\in\mathfrak{m}$，$x\in I$，即 $m=1+(-x)$，$-x\in I$，由(4)知 $m\in\mathfrak{m}$ 为可逆元，这是不可能的，故(4)成立时(1)必成立。 □

现在再证明一条与 K_0 群有关的引理。

引理 3.4 设 $\pi:R\twoheadrightarrow S$ 为环的满同态，$\mathrm{Ker}\pi=I$，$P\in$ f. g. $P_R\mathfrak{M}$，且记 $\bar{P}=P/IP$，则

$$K_0(\pi)([P])=[\bar{P}]$$

因此 $K_0\pi$ 由 $\mathrm{Ker}\pi$ 完全确定。

证 只需证 $S\underset{\pi}{\otimes}P\overset{S}{\simeq}\bar{P}$(作为左 S-模)。下面来证更强的结果：$S\underset{\pi}{\otimes}P\simeq\bar{P}$(作为左 S-模)。事实上，注意有环同构 $S\simeq R/I$，于是有${}_Z\mathfrak{M}_R$ 正合列

$$0\longrightarrow I\longrightarrow R\overset{\pi}{\longrightarrow}S\longrightarrow 0$$

注意 $P\in P_R\mathfrak{M}\subset\mathrm{Flat}_R\mathfrak{M}$(平坦左 R-模范畴)，以 $-\underset{R}{\otimes}P$ 作用于该正合列可得${}_Z\mathfrak{M}$ 正合列

$$0\longrightarrow I\underset{R}{\otimes}P\longrightarrow R\underset{R}{\otimes}P\longrightarrow S\underset{R}{\otimes}P\longrightarrow 0$$

而由 P 的平坦性知 $I\underset{R}{\otimes}P\simeq IP$，$R\underset{R}{\otimes}P\simeq P$(在${}_Z\mathfrak{M}$ 中)，于是有${}_Z\mathfrak{M}$ 中的同构

$$S\underset{R}{\otimes}P=S\underset{\pi}{\otimes}P\simeq P/IP=\bar{P},$$

$$(s=\pi(r)=\bar{r},x\in P\text{ 时},\bar{r}\otimes x\mapsto\overline{rx}=rx+IP)$$

再证这也是${}_S\mathfrak{M}$中的同构。事实上，$\forall\,\bar{r}、\bar{r}_1\in S$，$x\in P$，有

$$\bar{r}_1(\bar{r}\otimes x)=(r_1r+I)\otimes x=r_1r\otimes x+I\otimes x$$

视 $I\underset{R}{\otimes}P=IP$，$R\underset{R}{\otimes}P=P$，则有

$$\bar{r}_1(\bar{r}\otimes x)=r_1r\otimes x+Ix=r_1rx+Ix=\overline{r_1rx}=\bar{r}_1\cdot\overline{rx}$$

于是有${}_S\mathfrak{M}$ 同构 $S\underset{R}{\otimes}P\simeq\bar{P}$。 □

由引理 3.1(NAK 引理)与引理 3.4 可证明下述常用的结果。

定理 3.1 设 $\pi:R\twoheadrightarrow S$ 为环的满同态，$\mathrm{Ker}\pi=I\subseteq J(R)$，则 $K_0(\pi):K_0(R)\longrightarrow K_0(S)$为单同态，即在同构意义下 $K_0(R)$为 $K_0(S)$的子群(R，S 为交换环时也是子环)。

证 只需证在 $K_0(S)$中$[\bar{P}]=[\bar{Q}]$时在 $K_0(R)$中必有$[P]=[Q]$，其中 $P,Q\in$ f. g. $P_R\mathfrak{M}$，$\bar{P}=P/IP$，$\bar{Q}=Q/IQ$。为此只需证：${}_S\mathfrak{M}$ 中的同构 $\bar{P}\oplus S^n\simeq\bar{Q}\oplus S^n$ 蕴含着${}_R\mathfrak{M}$ 中的同构 $P\oplus R^n\simeq Q\oplus R^n$。为此又只需证：${}_S\mathfrak{M}$ 中的同构 $\bar{X}\simeq\bar{Y}$(其中 $X,Y\in$ f. g. $P_R\mathfrak{M}$)蕴含着有${}_R\mathfrak{M}$ 中的同构 $X\simeq Y$。

事实上，注意 $\bar{X}$ 的 S-模乘法为 $s\bar{x}=r\bar{x}$，其中 $\bar{x}\in X$，$\pi(r)=s\in S$，$r\in R$，记${}_S\mathfrak{M}$ 同构为 $\theta:\bar{X}\longrightarrow\bar{Y}$，则

$$\theta(r\bar{x}) = \theta(s\bar{x}) = s\theta(\bar{x}) = r\theta(\bar{x})$$

因此 θ 也是 $_R\mathfrak{M}$ 同构。

考察 $_R\mathfrak{M}$ 中的同态图（$\twoheadrightarrow$ 表满同态，$\rightarrowtail$ 表单同态 π_1,π_2 为标准同态）

由 $X\in P_R\mathfrak{M}$ 知有同态 $\tau: X\longrightarrow Y$ 使右图为交换图，我们先证 τ 为满同态。事实上，$\forall y\in Y$，由 $\pi_2\tau=\theta\pi_1$ 且 θ 与 π_1 满知必有 $y_1\in\tau(X)$ 使 $\pi_2(y)=\pi_2(y_1)$（$y\in\tau(X)$ 时 y,y_1 可相同）。于是

$$y = y_1 + (y - y_1) \in \tau(X) + \mathrm{Ker}\pi_2$$

因此

$$Y = \tau(X) + \mathrm{Ker}\pi_2 = \tau(X) + IY$$

但 $I\subseteq J(R)$，于是由 NAK 引理知 $Y=\tau(X)$，即 τ 为满同态。再注意 $Y\in P_R\mathfrak{M}$，由 τ 的满性又知必有 $_R\mathfrak{M}$ 中（单）同态 $i: Y\rightarrowtail X$ 使 $\tau i=I_Y$（可裂性）。故有

$$X = i(Y) \oplus \mathrm{Ker}\tau \tag{2}$$

又显然有

$$\mathrm{Ker}\tau \subset \mathrm{Ker}\pi_2\tau \xlongequal[\pi_2\tau=\theta\pi_1]{} \mathrm{Ker}\theta\pi_1 \xlongequal[\theta\text{为同构}]{} \mathrm{Ker}\pi_1 = IX$$

于是由(2)知

$$X = i(Y) + IX$$

再用 NAK 引理（注意 $X\in \mathrm{f.g.}\,_R\mathfrak{M}$）即知 $X=i(Y)$，因此(2)中的 $\mathrm{Ker}\tau=0$，即 τ 为单同态。但由上已知 τ 为满同态，故 $\tau: X\to Y$ 为 $_R\mathfrak{M}$ 中的同构。 □

由此定理可得两个有用的推论。

推论 3.1 设 $\pi: R\twoheadrightarrow S$ 为环的满同态且 $1+\mathrm{Ker}\pi\subseteq R^{\cdot}$（$R$ 的可逆元乘法群），则

(1) $K_0(\pi): K_0(R)\longrightarrow K_0(S)$ 为单同态；

(2) 若 $K_0(S)\in \mathrm{f.g.}\,_Z\mathfrak{M}$（f.g. AG），则 $K_0(R)$ 也是；

(3) 若 $S\in \mathrm{PSF}\cap\mathrm{IBN}$，则 $R\in\mathrm{PSF}\cap\mathrm{IBN}$（注意任意环同态 $f: R\longrightarrow S$，$S\in\mathrm{IBN}$ 时必有 $R\in\mathrm{IBN}$，见推论 2.1）。

注② 对任意环 R，定义 $\mathrm{rad}(R)$ 为 R 的一切素理想之交（也常记为 $N(R)$）称为 R 的**素根**（见§2）也称为**小根**。容易看出 $\mathrm{rad}(R)\subseteq J(R)$。由此可得下述推论：

推论 3.2 设 $\pi: R\twoheadrightarrow R/J(R)\equiv S$（或 $\pi: R\twoheadrightarrow R/\mathrm{rad}(R)\equiv S$）为标准环

同态，则推论 3.1 中的(1)、(2)、(3)仍成立。

由此也可看出：局部环都是 PSF 环(事实上是 PF 环)也是 IBN 环(注意除环为 IBN 环)。

注意在定理 3.1 中取 $S=R/J(R)$，当 R 为半局部环时，S 为半单 Artin 半环，即 $S\simeq D_1^{n_1\times n_1}\oplus\cdots\oplus D_k^{n_k\times n_k}$，其中 D_j 为除环，$j=1,\cdots,k$。于是

$$\mathrm{K}_0(S)\simeq\bigoplus_{j=1}^{k}\mathrm{K}_0(D_j^{n_j\times n_j})\simeq\bigoplus_{j=1}^{k}\mathrm{K}_0(D_j)\simeq\mathbb{Z}^k \tag{3}$$

且 $\mathrm{K}_0(R)\underset{\simeq}{<}\mathrm{K}_0(S)$，当 R 为交换半局部环时由中国剩余定理知，这个 k 正是 R 的极大理想个数。故立得本节的主要结果：

定理 3.2 设 R 为半局部环，则必有 $n\in\mathbb{N}$，使 $\mathrm{K}_0(R)\simeq\mathbb{Z}^n$，在 R 为交换环时这也是环同构，且对(3)中的 k，$n\leqslant k$。当 R 为交换半局部环时，k 为 R 的极大理想个数。

注③ 即使知道了(3)中的 k，这里的 n 仍难以确定。对此，[武同锁，1994]中得到了一个对确定半局部环的 K_0 群有意义的结果：$n=k\Leftrightarrow R$ 为半完全环。对交换的半局部环 R 确定这个 n 很有意义，因为此时 $R\in\mathrm{SFF}$(见[McDonald，1984])，因此 $R\in\mathrm{PF}\Leftrightarrow n=1$。$n$ 事实上是 R 与 PF 环差距的度量，以后将证：连通的交换半局部环必为 PF 环(当然 $n=1$，即 K_0 群与 $\mathbb{Z}$ 同构)。

从定理 3.2 与本节开头所述立得如下推论：

推论 3.3 设 R 为下列环类之一：左(右)Artin 环，半单 Artin 环，QF 环，左(右)完全环，半完全环，则 $K_0(\mathrm{R})\simeq\mathbb{Z}^n$，其中 $n\in\mathbb{N}$。

下面再将定理 3.2 作有意义的推广，为此先证两条引理：

引理 3.5 设 R 为交换环，A 为 R-代数且 $A\in\mathrm{f.g.}\,{}_R\mathfrak{M}$，则 $J(R)A\subseteq J(A)$，其中 $J(A)$ 为 A 作为环的 Jacobson 根。

证 注意，在引理 3.2 中对任意环 R，任意 $M\in{}_R\mathfrak{M}$，已得：$J(R)M\subseteq J(M)$。尽管 M 无极大子模时约定 $J(M)=M$，但对 $J(M)$，M 是作为 R-模的，这里的 $J(A)$ 中的 A 是作为 A-模给出的，不能直接引用。需另证如下：

任取 A 的极大左理想 M(记作 $M\underset{l,\max}{\lhd}A$)，只需证 $J(R)A\subseteq M$。

事实上，反设 $J(R)A\not\subset M$，则由 M 的极大性知

$$A=M+J(R)A$$

于是由 $A\in\mathrm{f.g.}\,{}_R\mathfrak{M}$ 知，用 NAK 引理即得 $M=A$，这与 $M\underset{l,\max}{\lhd}A$ 矛盾。故

$$J(R)A\subseteq M,\qquad\qquad \forall M\underset{l,\max}{\lhd}A$$

由此即知 $J(R)A\subseteq J(A)$。 □

引理 3.6 设 R 为交换半局部环，A 为 R-代数且 $A\in\mathrm{f.g.}\,{}_R\mathfrak{M}$，则 A 为

半局部环。

证 只需证明 $A/J(A)$ 为 Artin 环(即 $A/J(A)$ 作为(左)$A/J(A)$-模为 Artin 模)。

由引理 3.5 已知 $J(R)A\subseteq J(A)$，因此有环同态

$$R/J(R)\longrightarrow A/J(A)$$

再由 $A\in \text{f. g.}\,{}_R\mathfrak{M}$ 即知 $A/J(A)\in \text{f. g.}\,{}_{R/J(R)}\mathfrak{M}$。但由 R 为半局部环，可知 $R/J(R)$ 为 Artin 环。因此，作为 $R/J(R)$-模，$A/J(A)$ 为 Artin 模，于是，注意 $A/J(A)$ 的 $A/J(A)$-子模无穷降链也是其 $R/J(R)$-子模的无穷降链，即知 $A/J(A)$ 为 Artin 环。 □

由引理 3.6 立得定理 3.2 的下述推广。

定理 3.3 设 R 为交换半局部环，A 为 R-代数且 $A\in \text{f. g.}\,{}_R\mathfrak{M}$，则 $K_0(A)\simeq \mathbb{Z}^n$，其中 $n\in \mathbb{N}$。

此定理十分有用，比如由此定理立得如下推论：

推论 3.4 设 R 为交换半局部环，G 为有限群，则 $K_0(RG)\simeq \mathbb{Z}^n$，其中 $n\in \mathbb{N}$。

注④ 由上可知半局部环的 K_0 群都是有限生成的。事实上，判定一个环的 K_0 群的有限生成性十分重要，因为若能断言定理 3.1 及命题 2.5 中环 S 的 K_0 群是有限生成的，则可估计出 $K_0(R)$ 的结构(由有限生成 Abel 群的结构定理)。令人遗憾的是：这是一个十分艰难的问题，因为现在已知：任一个以 $\mathbb{Z}$ 作直和项的 Abel 群都可作为某一个 Dedekind 环的 K_0 群(见[Claborn 1966])。因此，即使对 Dedekind 环，K_0 群也未必是有限生成的，此外对环同态 $f:R\to S$，确定 $K_0(f)$ 的满单性当然也是重要的。为此，"在理论上"我们易得如下结果：

命题 3.1 设 $f:R\to S$ 为环同态，则

(1) $K_0(f)$ 为满同态$\Leftrightarrow \forall\, Q\in \text{f. g. P}_S\mathfrak{M}$，有 $n\in \mathbb{N}$ 与 $P\in \text{f. g. P}_R\mathfrak{M}$ 使得 $S\otimes_R P\simeq Q\oplus S^n$；

(2) $K_0(f)$ 为单同态$\Leftrightarrow \forall\, P,P'\in \text{f. g. P}_R\mathfrak{M}$，$S\otimes_R P\overset{S}{\simeq} S\otimes P'$ 当且仅当 $P\overset{S}{\simeq} P'$。

在一些重要情况下，本节上一部分与前节事实上是由环同态 $f:R\to S$ 决定的 $K_0(f)$ 的单性(即 $\text{Ker}\,K_0(f)=0$)推断出 $K_0(S)$ 同构于 $K_0(R)$ 的一个子群从而给出一些有意义的结果。下面转向 $\text{Coker}\,K_0(f)\equiv K_0(R)/\text{Im}(K_0(f))$(刻画着 $K_0(f)$ 满的程度)的研究。

注意，对任一环 R 都存在(惟一)环同态 $f:\mathbb{Z}\to R$，对这个通用的环同

态，我们给出如下定义：

定义 3.2 对环同态 $f:\mathbb{Z}\to R$，称

$$\widetilde{\mathrm{K}}_0(R)\equiv \mathrm{K}_0(R)/\mathrm{Im}\mathrm{K}_0(f)\equiv \mathrm{Coker}\ \mathrm{K}_0(f)$$

为环 R 的 **Grothendieck 约化群**(reduced group)，简称为 R 的**约化群或投射类群**(projective class group)。

先证明下述的简单结果：

命题 3.2 对环同态 $f:\mathbb{Z}\to R$，$\mathrm{Im}\mathrm{K}_0(f)=\mathbb{Z}[R]$为 $\mathrm{K}_0(R)$由$[R]$生成的循环子群(当 $R\in\mathrm{IBN}$ 时 $\mathrm{Im}\mathrm{K}_0(f)\simeq\mathbb{Z}$)。因此

$$\widetilde{\mathrm{K}}_0(R)=\mathrm{K}_0(R)/\mathbb{Z}[R]$$

证 由§2 知，$\mathrm{K}_0(f)([P])=[R\otimes_{\mathbb{Z}}P]$，$\forall P\in \mathrm{f.g.P}_{\mathbb{Z}}\mathfrak{M}$，但$\mathbb{Z}\in\mathrm{PID}$，于是 $P\in \mathrm{f.g.Free}_{\mathbb{Z}}\mathfrak{M}$，即有 $n\in\mathbb{N}$ 使 $P\simeq\mathbb{Z}^n$，由此知

$$\mathrm{K}_0(f)([P])=[R\otimes_{\mathbb{Z}}\mathbb{Z}^n]=n[R\otimes_{\mathbb{Z}}\mathbb{Z}]=n[R]$$

由此即知 $\mathrm{Im}\mathrm{K}_0(f)=\mathbb{Z}[R]$。故由定义知

$$\widetilde{\mathrm{K}}_0(R)=\mathrm{K}_0(R)/\mathbb{Z}[R]$$ □

推论 3.5 环 $R\in\mathrm{PSF}\Leftrightarrow\widetilde{\mathrm{K}}_0(R)=0$，因此 $\widetilde{\mathrm{K}}_0(R)$是 R 与 PSF 环差距的度量。

证 由命题 1.6 与命题 3.2 即得。 □

命题 3.3 设环 $S\in\mathrm{PSF}\cap\mathrm{IBN}$ 且有环同态 $g:R\to S$，则 $R\in\mathrm{IBN}$ 且对环同态 $f:\mathbb{Z}\to R$，有 Abel 群分解

$$\begin{aligned}\mathrm{K}_0(R)&=\mathrm{Im}\mathrm{K}_0(f)\oplus\mathrm{Ker}\ \mathrm{K}_0(g)\\&=\mathbb{Z}[R]\oplus\mathrm{Ker}\mathrm{K}_0(g)\simeq\mathbb{Z}\oplus\widetilde{\mathrm{K}}_0(R)\end{aligned}$$

证 由推论 2.1 可知 $R\in\mathrm{IBN}$，因此 $\mathrm{Im}\mathrm{K}_0(f)=\mathbb{Z}[R]\simeq\mathbb{Z}$。再用函子 K_0 作用交换图

$$\begin{array}{ccc}\mathbb{Z}&\xrightarrow{f}&R\\&\searrow^{gf}&\downarrow g\\&&S\end{array}$$

得交换图

$$\begin{array}{ccc}\mathbb{Z}\cong\mathrm{K}_0(\mathbb{Z})&\xrightarrow{\mathrm{K}_0 f}&\mathrm{K}_0(R)\\&\searrow^{\mathrm{K}_0(g)\mathrm{K}_0(f)}&\downarrow\mathrm{K}_0(g)\\&&\mathrm{K}_0(S)\cong\mathbb{Z}\\&&\text{命题1.7}\\&&[S]\mapsto 1\end{array}$$

由此知 $\mathrm{K}_0(g)\mathrm{K}_0(f)$ 为 $_{\mathbb{Z}}\mathfrak{M}$(AG)同构。因此 $\mathrm{K}_0(g)$ 为满同态，$\mathrm{K}_0(f)$ 为单同态。

任取 $x\in\mathrm{K}_0(R)$，若 $x\notin\mathrm{Im}\mathrm{K}_0(f)$，则由 $\mathrm{K}_0(g)\mathrm{K}_0(f)$ 为满同态知必有 $x_1\in\mathrm{Im}\mathrm{K}_0(f)$ 使 $\mathrm{K}_0(g)(x)=\mathrm{K}_0(g)(x_1)$，即 $x-x_1\in\mathrm{Ker}\mathrm{K}_0(g)$，于是由 $x=x_1+(x-x_1)$ 知 $\mathrm{K}_0(R)=\mathrm{Im}\mathrm{K}_0(f)+\mathrm{Ker}\mathrm{K}_0(g)$。另一方面由 $\mathrm{K}_0(g)\mathrm{K}_0(f)$ 为单同态又知

$$\mathrm{Im}\mathrm{K}_0(f)\cap\mathrm{Ker}\mathrm{K}_0(g)=0$$

因此

$$\mathrm{K}_0(R)=\mathrm{Im}\mathrm{K}_0(f)\oplus\mathrm{Ker}\mathrm{K}_0(g)=\mathbb{Z}[R]\oplus\mathrm{Ker}\mathrm{K}_0(g)$$

再由

$$\mathrm{Ker}\mathrm{K}_0(g)\simeq\mathrm{K}_0(R)/\mathrm{Im}\mathrm{K}_0(f)=\widetilde{\mathrm{K}}_0(R)$$

即知

$$\mathrm{K}_0(R)\simeq\mathbb{Z}\oplus\widetilde{\mathrm{K}}_0(R)$$ □

注⑤ 命题 3.3 中给出的 $\mathrm{K}_0(R)$ 的直和分解与 S 及 g 的选取有关，见下例。

例 1 设 $R=\mathbb{Z}\oplus\mathbb{Z}$，$S=\mathbb{Z}$，取两个环同态

$$g_1:\ R\longrightarrow S \qquad\qquad g_2:\ R\longrightarrow S$$
$$(x,y)\longmapsto x\ , \qquad\qquad (x,y)\longmapsto y$$

则

$$\mathrm{Ker}\mathrm{K}_0(g_1)=\mathbb{Z}[(0,\mathbb{Z})],$$
$$\mathrm{Ker}\mathrm{K}_0(g_2)=\mathbb{Z}[(\mathbb{Z},0)]$$

因此

$$\mathrm{K}_0(R)=\mathbb{Z}[\mathbb{Z}\oplus\mathbb{Z}]\oplus[(0,\mathbb{Z})]=\mathbb{Z}[\mathbb{Z}\oplus\mathbb{Z}]\oplus\mathbb{Z}[(\mathbb{Z},0)]$$

注⑥ 当 R 不是交换环时，$\mathbb{Z}$ 未必同构于 $\mathrm{K}_0(R)$ 的直和项(见§1，例 1 即知)。事实上，[Goodearl,1991]给出的例子说明：$\forall n\in\mathbb{N}$，都有 von Neumann 正则环 R 使，$\mathrm{K}_0(R)\simeq\mathbb{Z}/n\mathbb{Z}\cong\mathbb{Z}_n$，甚至有 von Neumann 正则环 R 使 $\mathrm{K}_0(R)\simeq\mathbb{R}$(实数加群)。

将命题 3.3 用于交换环可得一个常用的结果。

定理 3.4 设 R 为交换环，则有 Abel 群同构

$$\mathrm{K}_0(R)\simeq\mathbb{Z}\oplus\widetilde{\mathrm{K}}_0(R)$$

证 由 R 为交换环知，任取 R 的极大理想 $\mathfrak{m}$，则 $R/\mathfrak{m}=F$ 为域，当然 $F\in\mathrm{PSF}\cap\mathrm{IBN}$。在命题 3.3 中取 $S=F$，$g=\pi:R\twoheadrightarrow F$ 为标准同态(由此知：对交换环，命题 3.3 中的 S 与 g 必存在)，仍取 $f:\mathbb{Z}\to R$，即得证。 □

由定理 3.4 知，对交换环的 K_0 群的研究与计算可归为约化群的研究与计算。以后我们将证明：对 Dedekind 环 R，$\widetilde{K}_0(R)$ 与 R 的 Picard 群 Pic(R) 以及 R 的理想类群 $Cl(R)$ 都是同构的，它们的大小是 Dedekind 环与 UFD(也是与 PID)差距的度量。[Claborn，1966]证出：对任意的 Abel 群 G，必有一个 Dedekind 环 R 使 $\widetilde{K}_0(R)\simeq G$。但对代数数域($\mathbb{Q}$ 的有限扩张域)中的代数整元环这种特殊的 Dedekind 环，我们以后将证 $\widetilde{K}_0(R)$ ($Cl(R)$)为有限群，其阶数(元素个数)称为该代数数域的类数。对这种类数的研究已成为代数数论中的重要课题之一，至今仍有一些艰难问题未获解决，仍在继续进行中。

约化群在拓扑与代数上的另一个有趣的应用可简介如下(在 § 14 中我们将再作系统地介绍)。设 B 为紧致的 Hausdorff 空间，从引言中我们已知 $K^0(B)\simeq K_0(C(B))$，其中 $K^0(B)$ 为 B 上向量丛同构类的半群 Vec(B) 的群完备化，$C(B)$ 为 B 上的实(复)连续函数环。设 B 是连通的，则 Vec(B) 中的任一元素 $[X]$ 都对应一个确定的维数，记为 $\dim[X]$，令 $\varepsilon: K^0(B)\to\mathbb{Z}$ 使 $\varepsilon([X])=\dim[X]$，则 ε 为一个 Abel 群的满同态，记 $\operatorname{Ker}\varepsilon$ 为 $\widetilde{K}^0(B)$。可以看出 $\widetilde{K}^0(B)\simeq\widetilde{K}_0(C(B))$。而 Bott 周期性定理断言，对 n 维球面 S^n，

$$\widetilde{K}^0(S^n)=\begin{cases}\mathbb{Z}/2\mathbb{Z}=\mathbb{Z}_2, & n\equiv 1,\ 2\pmod 8\\ \mathbb{Z}, & n\equiv 0,4\pmod 8\\ 0, & n=3,5,6,7\pmod 8\end{cases}$$

据此可证实数域上的可除代数恰有四种：实数域、复数域、四元数体(非交换代数)与 Cayley 的八元数代数(非结合代数)(可参看[Hirzebruch，1991])。

§ 4　局部秩与 K_0 群

对 IBN 环(如交换环与左(右)Noether 环)R 上的有限生成自由模 M，在 § 1 中我们已用过秩的概念(并由此在证明中定义过稳定自由模的秩)，这是一般抽象代数(近世代数)中都被定义过的，即 $M\simeq R^n$ 时规定 M 的秩 $\operatorname{rank}M=n$，由于 K_0 群立足于有限生成投射模，将秩的概念推广到有限生成投射模是十分必要的。

本节中的环都指交换环，即 CRing 中的环，对 $R\in$ CRing，记 Spec$R$ 为 R 的素理想集，称为 R 的素谱。

任给交换环 R 与非零的环同态 $0\neq g: R\to F$，其中 F 为域(比如取 P 为 R 的素理想，即 $P\in\operatorname{Spec}R$，令 F 为整环 R/P 的分式域(全商环)$Q(R/P)$ 即

可),则 $\mathrm{Im}g \simeq R/\mathrm{Ker}g < F$,因此 $\mathrm{Im}g$ 为整环,于是 $\mathrm{Ker}g \in \mathrm{Spec}R$。反过来,任取 $P \in \mathrm{Spec}R$,则标准环同态 $\pi: R \longrightarrow R/P < F = Q(R/P)$ 可看成是环同态 $0 \neq g: R \longrightarrow F$ 且 $\mathrm{Ker}g = P \in \mathrm{Spec}R$。于是在不考虑扩域时可以认为

$$\mathrm{Spec}R \xrightarrow{1-1} \{0 \neq g: R \longrightarrow F(\text{域})\}$$

由于 $\mathrm{K}_0(F) \simeq \mathbb{Z}[F] \simeq \mathbb{Z}$ 可看作是 $\mathrm{K}_0(F) = \mathbb{Z}$,于是对任意的 $M \in \mathrm{f.g.P}_R\mathfrak{M}$,$\mathrm{K}_0(g)([M]) = [F \bigotimes_R M] \in \mathbb{Z}$。但 $F \bigotimes_R M \in {}_F\mathfrak{M}$($F$ 上的线性空间)必有确定的维数 $\dim_F F \bigotimes_R M \in \mathbb{Z}$,于是可作如下定义:

定义 4.1　设 $R \in \mathcal{C}\mathrm{Ring}$,$M \in \mathrm{f.g.P}_R\mathfrak{M}$,$P \in \mathrm{Spec}R$,$g: R \longrightarrow F = Q(R/P)$,则称 $\dim_F F \bigotimes_R M$(即 $\mathrm{K}_0(g)([M])$)为 M 在素理想 P 的**局部秩**(local rank)记为 $\mathrm{rank}_P M$。

对一般的整环 R 与 $M \in {}_R\mathfrak{M}$(未必有限生成,也未必投射)记 $F = Q(R/0) = Q(R)$,可定义 M 的秩 $\mathrm{rank}M = \dim_F F \bigotimes_R M$,当 $M \in \mathrm{f.g.P}_R\mathfrak{M}$ 时,这个秩即定义 4.1 中的 $\mathrm{rank}_P M$ 的公共值,与 P 无关。为什么会有这种断言,读完命题 4.6 与命题 4.7 即知。

由定义 4.1 可看出局部秩与 K_0 群有密切的关系,而研究局部秩的最有效的方法是局部化方法,下面先简要地介绍环与模的局部化。

设 $R \in \mathcal{C}\mathrm{Ring}$,$S$ 为 R 中的一个乘法封闭(子)集,即 $1 \in S$ 且 S 对 R 的乘法封闭(因此 S 对 R 的乘法为幺半群)。在 Descartes 积

$$S \times R = \{(s, r) \mid s \in S, r \in R\}$$

上定义一个关系(对比 §1 中半群的群完备化):

$$(s, r) \sim (s_1, r_1) \Leftrightarrow \text{有 } t \in S \text{ 使 } tsr_1 = ts_1r$$

由此知若 $0 \in S$,则 $\sim$ 为平庸关系,又在 R 无零因子时,t 的要求可省去而以 $sr_1 = s_1r$ 来定义。显然这是 $S \times R$ 上的一个等价关系,记 $\frac{r}{s}$ 为含 (s, r) 的等价类,且记

$$S^{-1}R = \left\{\frac{r}{s} \mid s \in S,\ r \in R\right\}$$

按分数运算定义 $S^{-1}R$ 中的加、乘运算,则 $S^{-1}R \in \mathcal{C}\mathrm{Ring}$,$\frac{0}{1}$ 为零元,$\frac{1}{1}$ 为单位元,仍分别记为 0,1。(不要求 $1 \in S$ 时,$\frac{r}{r}$($0 \neq r \in S$)都是单位元。可证:此时所得的环与上述的 $S^{-1}R$ 同构)。$r \in S$ 时 $\left(\frac{r}{s}\right)^{-1} = \frac{s}{r}$(因此 $S^{-1}R$ 中可

逆元“增多”，$S^{-1}R$ 的结构性质可望比 R 更强)，这个 $S^{-1}R$ 被称为 R 在 S 上的**局部化**(localization)。

最常用的乘法封闭集有：① 当 $P\in \mathrm{Spec}R$ 时，$S=R\backslash P$(在代数几何中研究曲线、曲面的局部性质以及代数数论中研究素元的局部性质时都会用到)；② $0,1\neq f\in R$，$S=\{1,f,f^2\cdots\}$(代数几何中刻画正则函数时即会用到)。① 给出的局部化又常记为 R_P，称为 R 在 P 的局部化；② 给出的局部化则常记为 R_f。

容易直接验证如下结果。

引理 4.1 设 $R\in \mathcal{C}\mathrm{Ring}$，则

(1) 有标准(自然)环同态 $\sigma:R\longrightarrow S^{-1}R$ 使 $\sigma(r)=\frac{r}{1}$，$\forall r\in R$，且

$$\mathrm{Ker}\sigma=\{r\in R\mid 有\ t\in S\ 使\ tr=0\}$$

因此当且仅当 S 中无(R 中的)零因子时，σ 为单同态，此时 $S^{-1}R$ 可看作 R 的扩环；

(2) 设 S 为 R 的全体非零因子集合(比如当 R 为整环时，$S=R\backslash 0$)，则 $S^{-1}R=Q(R)$(R 的全商环，R 为整环时，即 R 的分式域)。

引理 4.2 设 $R\in \mathcal{C}\mathrm{Ring}$，$S$ 为 R 中不含 0 的乘法封闭集，则 $\forall s\in S$，s 在标准同态 σ 下的象 $\sigma(s)$ 在 $S^{-1}R$ 中可逆且 $\sigma:R\longrightarrow S^{-1}R$ 有如下泛性质：对任意环同态 $f:R\longrightarrow \bar{R}$，若对任意的 $s\in S$，$f(s)$ 在 $\bar{R}$ 中都是可逆的，则有惟一的环同态 $\bar{f}:S^{-1}R\longrightarrow \bar{R}$ 使 $\bar{f}(\frac{r}{1})=f(r)$，$\forall r\in R$，即 $f=\bar{f}\sigma$。

由关于泛性质的常规证法(参看引理 1.1 之证)可得：

命题 4.1 设 $R\in \mathcal{C}\mathrm{Ring}$，$S$ 为 R 的乘法封闭集，则 $S^{-1}R$ 在同构意义下存在惟一。

环的局部化可推广为模的局部化，设 $M\in {}_R\mathfrak{M}$，以 $S\times M$ 代替前面的 $S\times R$，仿前定义，即 $(s_1,m_1)\sim(s_2,m_2)\Leftrightarrow$ 有 $t\in S$ 使 $ts_2m_1=ts_1m_2$，$\forall s_1,s_2\in S$，$m_1,m_2\in M$。记 $\frac{m}{s}$ 为 (s,m) 所在的等价类，$S^{-1}M=\left\{\frac{m}{s}\mid s\in S,m\in M\right\}$ 且在 $S^{-1}M$ 中，规定运算

$$\frac{m_1}{s_1}+\frac{m}{s}=\frac{sm_1+s_1m}{s_1s},$$

$$\frac{r_1}{s_1}\cdot\frac{m}{s}=\frac{r_1m}{s_1s},\qquad \forall r_1\in R,s,s_1\in S,m,m_1\in M$$

则 $S^{-1}M\in {}_{S^{-1}R}\mathfrak{M}$，称为 M 在 S 上的**局部化**。当 $S=R\backslash P$，$P\in \mathrm{Spec}R$ 时，也

常记为 M_P，称为 M 在 P 的局部化。

有趣的是，通过标准环同态 $\sigma: R \longrightarrow S^{-1}R$ 可证如下结果：

命题 4.2　设 $R \in \mathcal{C}\mathrm{Ring}$，$S$ 为 R 中的乘法封闭集，$\sigma: R \longrightarrow S^{-1}R$ 为标准环同态，$M \in {}_R\mathfrak{M}$，则有 $S^{-1}R$-模同构

$$S^{-1}M \simeq S^{-1}R \underset{\sigma}{\otimes} M = S^{-1}R \underset{R}{\otimes} M$$

证　定义

$$\varphi: S^{-1}R \times M \to S^{-1}M$$

$$(\frac{r}{s}, m) \mapsto \frac{rm}{s}$$

易见 φ 为 R-双线性映射。因此由 $\otimes$ 的泛性质知，必有 ${}_{S^{-1}R}\mathfrak{M}$ 同态

$$f: S^{-1}R \underset{\sigma}{\otimes} M \to S^{-1}M$$

使 $\varphi = f\otimes$。下证 f 为 ${}_{S^{-1}R}\mathfrak{M}$ 同构。事实上 f 显然为满同态，只需证 f 为单同态，注意 $S^{-1}R \underset{\sigma}{\otimes} M = S^{-1}R \underset{R}{\otimes} M$ 的元素都可表为

$$\begin{aligned}\sum_{j=1}^{n} \frac{r_j}{s_j} \otimes m_j &= \frac{1}{s_1 s_2 \cdots s_n}(s_2 \cdots s_n r_1 \otimes m_1 + s_1 s_3 \cdots \\ &\qquad s_n r_2 \otimes m_2 + \cdots + s_1 s_2 \cdots s_{n-1} r_n \otimes m_n) \\ &= \frac{1}{s_1 s_2 \cdots s_n}(1 \otimes s_2 s_3 \cdots s_n r_1 m_1 \\ &\qquad + 1 \otimes s_1 s_3 \cdots s_n r_2 m_2 + \cdots + 1 \otimes s_1 s_2 s_3 \cdots s_{n-1} r_n m_n) \\ &= \frac{1}{s} \otimes m\end{aligned}$$

其中 $s = s_1 s_2 \cdots s_n \in S$，而

$$m = s_2 s_3 \cdots s_n r_1 m_1 + s_1 s_3 \cdots s_n r_2 m_2 + \cdots + s_1 s_2 s_3 \cdots s_{n-1} r_n m_n \in M。$$

若 $f(\frac{1}{s} \otimes m) = 0$，即 $\frac{m}{s} = 0$，则有 $t \in S$ 使 $tm = 0$，于是

$$\frac{1}{s} \otimes m = \frac{t}{ts} \otimes m = \frac{1}{ts} \otimes tm = 0$$

由此知 $\mathrm{Ker} f = 0$，即 f 为单同态，从而为同构。　□

由此命题知，可记 $S^{-1}M = S^{-1}R \underset{R}{\otimes} M$，不难验证

$$S^{-1}: {}_R\mathfrak{M} \to {}_{S^{-1}R}\mathfrak{M}$$

为共变函子，且由张量积性质知 S^{-1} 还是右正合函子。再注意，任取 ${}_R\mathfrak{M}$ 中单同态 $g: M \to N$，则

$$S^{-1}(g) = 1 \otimes g: S^{-1}R \underset{R}{\otimes} M \to S^{-1}R \underset{R}{\otimes} N$$

若 $S^{-1}(g)(\frac{1}{s}\otimes m)=0$，即 $\frac{1}{s}\otimes g(m)=0$。于是 $f(\frac{1}{s}\otimes g(m))=\varphi\left(\frac{1}{s},g(m)\right)=\frac{g(m)}{s}=0$。由此知，有 $t\in S$ 使 $tg(m)=0$，即 $g(tm)=0$。但 g 为单同态，因此 $tm=0$，故 $\frac{1}{s}\otimes m=\frac{m}{s}=0\in S^{-1}M=S^{-1}R\underset{R}{\otimes}M$，即 $S^{-1}g$ 为单同态，又容易看出 S^{-1} 保直和，因此 $S^{-1}(\mathrm{P}_R\mathfrak{M})\subset \mathrm{P}_{S^{-1}R}\mathfrak{M}$。由此即得

命题 4.3 设 $R\in \mathrm{CRing}$，S 为 R 中的乘法封闭集，则 $S^{-1}R\in \mathrm{Flat}_R\mathfrak{M}$，因此 $S^{-1}:{}_R\mathfrak{M}\to{}_{S^{-1}R}\mathfrak{M}$，$S^{-1}:\mathrm{P}_R\mathfrak{M}\to \mathrm{P}_{S^{-1}R}\mathfrak{M}$，$S^{-1}:\mathrm{f.g.\,P}_R\mathfrak{M}\longrightarrow \mathrm{f.g.\,P}_{S^{-1}R}\mathfrak{M}$ 都为正合共变函子。

当 $P\in \mathrm{Spec}R$，$S=R\backslash P$ 时，常记 $g_P=S^{-1}(g)$，$\forall g:M\to N$（${}_R\mathfrak{M}$ 中的同态）。由命题 4.2 知 $M_P\simeq R_P\underset{R}{\otimes}M$，注意 $P\in{}_R\mathfrak{M}$，$PR_P=P_P=\{\frac{x}{y}\mid x\in P,y\in R\backslash P\}\lhd R_P$。任取 $r\in R$，$s\in S=R\backslash P$，若 $\frac{r}{s}\notin P_R$，则 $r\notin P$，因此 $r\in S$，于是 $\frac{r}{s}\in R_p^{\cdot}$。由此知 $R_P=P_p\dot{\cup}R_p^{\cdot}$，故得如下结果。

命题 4.4 设 $R\in \mathrm{CRing}$，$P\in \mathrm{Spec}R$，则 R_P 为交换局部环，其惟一极大理想为 $PR_P=P_P$ 且 $\mathrm{K}_0(R_P)\simeq\mathbb{Z}$，因此

$$\mathrm{K}_0(R)\simeq \mathrm{K}_0(R_P)\oplus\widetilde{\mathrm{K}}_0(R),\ \forall P\in \mathrm{Spec}R$$

通常带惟一极大理想 $\mathfrak{m}$ 的交换局部环 R，常记为 $(R,\mathfrak{m})$，且称 $R/\mathfrak{m}$ 为 R 的剩余类域。现在来证下述引理，它说明交换环 R 在素理想 P 的局部化 R_P 的剩余类域可看作是 R/P 的全商环（分式域）。

引理 4.3 设 $R\in \mathrm{CRing}$，$P\in \mathrm{Spec}R$，则

$$F\equiv Q(R/P)\simeq R_P/P_P$$

证 记 $\sigma:R\longrightarrow R_P$ 为标准环同态，$\pi:R\twoheadrightarrow R/P$ 为（关于商环的）标准环同态，$i:R/P\longrightarrow F$ 为嵌入同态，考虑下图

$$\begin{array}{ccc} R & \xrightarrow{\sigma} & R_P \\ {\scriptstyle\pi}\downarrow & \searrow^{i\pi} & \downarrow{\scriptstyle h\exists 1} \\ R/P & \xrightarrow[i]{} & F \end{array} \qquad (1)$$

$\forall x\notin P$，即 $x\in S=R\backslash P$，$i\pi(x)$ 均为 F 中的可逆元。于是由局部化的泛性质知，有惟一的环同态 $h:R_P\longrightarrow F$ 使上图为交换图，下面只需证 h 满且

$\mathrm{Ker}h=P_P$。

事实上，$\forall r\in R$，记

$$\bar{r}=h(\frac{r}{1})=h(\sigma(r))=i\pi(r)$$

当 $r\notin P$ 即 $r\in S$ 时，

$$h(\frac{1}{r})\cdot h(\frac{r}{1})=h(\frac{1}{r}\cdot\frac{r}{1})=h(\frac{1}{r})\bar{r}=h(1)=1\in F$$

即 $\bar{r}$，$\bar{r}^{-1}=h(\frac{1}{r})\in F^{\cdot}=F\backslash 0$。而 $F^{\cdot}$ 的元素都可表为 $\bar{r}_1\bar{r}_2^{-1}$ 形，其中 $r_1,r_2\in S$，于是 $F^{\cdot}\in\mathrm{Im}h$，因此 $F=\mathrm{Im}h$（注意 $0\in\mathrm{Im}h$），即 h 为满同态。当 $r\in P$ 时，$0=i\pi(r)=h(\frac{r}{1})$，因此 $\mathrm{Ker}h=P_P$。故 $F\simeq R_P/P_P$。 □

由此引理可证：

命题 4.5　设 $R\in \mathrm{CRing}$，$P\in\mathrm{Spec}R$，则对(1)中的 $h:R_P\to F$，

$$\mathrm{K}_0(h):\mathrm{K}_0(R_P)\to\mathrm{K}_0(F)$$

为群(环)同构。事实上即 的自同构，因此 $M\in \mathrm{f.g.P}_R\mathfrak{M}$ 的局部秩 $\mathrm{rank}_P M$ 就是 M 在 P 的局部化 M_p 的秩，即

$$\mathrm{rank}_P M=n\Leftrightarrow M_P\simeq R_P^n$$

证　注意 R_P 为交换局部环，$J(R_P)=P_P=\mathrm{Ker}h$，$\mathrm{K}_0(R_P)\simeq$ $\simeq\mathrm{K}_0(F)$，$\mathrm{K}_0(h)([R_P])=[F\otimes_{R_P}R_P]=[F]\neq 0$，由上节定理 3.1 即知 $\mathrm{K}_0(h)$ 为同构。再注意 R_P 为局部环，即知 $\mathrm{rank}_P M=n$ 等价于 $M_P\simeq R_P^n$。 □

注①　对环 R 作局部化 R_P 实质上起着三个作用：(a) P 外的(即含 P 的)素理想(即与 $S=R\backslash P$ 相交的素理想)全变为 R_P，不再是 R_P 的素理想，因此 R_P 的素理想比 R 的更少；(b) P 内的素理想仍保持包含关系地保留着；(c) $S=R\backslash P$ 中即 P 外的元素均变成 R_P 中的可逆元，P_P 为 R_P 的惟一极大理想。因此 $R_P=R_p^{\cdot}\dot{\cup}P_p$，可逆元增多常使环性质增多。所以对局部整体性质(一个性质 ，若被一切 R_P 具有时($\forall P\in\mathrm{Spec}R$)可保证 R 具有 ，则称 为局部整体性质)的研究(代数学本身，代数几何，代数数论中常用)十分重要。对一般乘法封闭集 S 上的局部化 $S^{-1}R$，也有类似的作用，即与 S 相交的素理想消失，与 S 不相交的素理想保持包含关系地保留着；S 中的元素都成为 $S^{-1}R$ 的可逆元。

下面我们来证一个有举足轻重地位的命题。

命题 4.6　设 $R\in \mathrm{CRing}$，$P_1,P_2\in\mathrm{Spec}R$ 且 $P_2\subset P_1$，$M\in \mathrm{f.g.P}_R\mathfrak{M}$，则

$$\mathrm{rank}_{P_1}M=\mathrm{rank}_{P_2}M$$

证 记 $S_i = R \backslash P_i$，由 $P_2 \subset P_1$ 知 $S_1 \subset S_2$，因此标准同态 $\sigma_2: R \to R_{P_2}$ 使 $\sigma_2(S_1) \subset R_{P_2}^{\cdot}$。于是由局部化的泛性质(引理 4.2)知，必有环同态 $\varphi: R_{P_1} \to R_{P_2}$ 使右图为交换图(其中 σ_1 也是标准环同态)：

$$\begin{array}{ccc} R & \xrightarrow{\sigma_1} & R_{P_1} \\ {\scriptstyle \sigma_2}\downarrow & \swarrow{\scriptstyle \varphi} & \\ R_{P_2} & & \end{array}$$

但 R_{P_1}，R_{P_2} 都是局部环，它们的 K_0 群都是(同构于)$\mathbb{Z}$。因此

$$K_0(\varphi): K_0(R_{P_1}) \to K_0(R_{P_2})$$

为同构且 $K_0(\varphi)([R_{P_1}]) = [R_{P_2}]$，再注意局部环上的有限生成投射模都是自由的即得 $\text{rank}_{P_1} M = \text{rank}_{P_2} M$。 □

这条命题用于两种极端情况——整环与交换局部环的情况，十分有效。因为在整环 R 中，$0 \in \text{Spec}R$，对 $\forall P \in \text{Spec}R$ 当然有 $0 \subset P$，此时由命题 4.6 知：$\forall M \in \text{f. g. P}_R\mathfrak{M}$，$\text{rank}_0 M$ 为一切 $\text{rank}_P M$ 的公共值。而当 R 为交换局部环时，其惟一极大理想 $\mathfrak{m}$ 包含着 R 的一切素理想，此时 $\text{rank}_{\mathfrak{m}} M$ 为一切 $\text{rank}_P M$ 的公共值。为写出这两个结论，我们先给出如下定义：

定义 4.2 设 $R \in \mathcal{C}\text{Ring}$，$M \in \text{f. g. P}_R\mathfrak{M}$，若对任意的 $P \in \text{Spec}R$ 都有 $\text{rank}_P M = n$，则称 M 有常数秩 n，记为 $\text{rank}M = n$。

例如，一切稳定自由模都有常数秩(请读者自证)。

命题 4.7 设 R 为整环或交换局部环，$M \in \text{f. g. P}_R\mathfrak{M}$，则 M 必有常数秩。

由此命题知：线性空间的维数理论的一些结果常可推广到整环上的有限生成投射模(未必自由)。至于对交换局部环，命题 4.7 事实上是前面的已知结果，因为此时有限生成投射模都是自由的且局部环为 IBN 环，线性空间维数理论的更大一部分可推广到交换局部环上的有限生成投射模。

由于任一素理想必含于某一极大理想之中，由命题 4.6 又可得如下命题：

命题 4.8 设 $R \in \mathcal{C}\text{Ring}$，$M \in \text{f. g. P}_R\mathfrak{M}$，则

$$\text{rank}M = n \Leftrightarrow \text{rank}_P M = n, \qquad \forall P \in \text{Max}R$$

其中 $\text{Max}R$ 为 R 的极大理想集，称为 R 的**极大谱**。

为了再深入地研究局部秩与常数秩，先在 $\text{Spec}R$ 上建立一个拓扑(称为 Zariski 拓扑)，即规定 $\text{Spec}R$ 中的闭集为 $V(A) = \{P \in \text{Spec} \mid P \supseteq A \lhd R\}$。显然，$V(A)$ 的余集(补集)为 $D(A) = \bigcup_{f \in A} \{P \in \text{Spec}R \mid f \notin P\}$，记 $D(r) = \{P \in \text{Spec}R \mid r \notin P\}$，则 $\text{Spec}R$ 有开集基 $\{D(r) \mid r \in R\}$。任取 $\text{Spec}R$ 的一族开覆盖 $\{D(r_j)\}_{j \in J}$，若有 $B \overset{\lhd}{\neq} R$ 使 B 由 $\{r_j\}_{j \in J}$ 生成，则必有 $\mathfrak{m} \in \text{Max}R \subset \text{Spec}R$ 使 $B \subset \mathfrak{m}$，即 $\mathfrak{m} \notin \bigcup_{j \in J} D(r_j)$，这与 $\{D(r_j)\}_{j \in J}$ 为 $\text{Spec}R$ 的开覆盖矛盾。

由此知 R 的单位元 1 必可由有限个 r_j 生成即 $\{D(r_j)\}_{j\in J}$ 必有一个有限子覆盖将 Spec$R$ 盖住，于是 Spec$R$ 为紧致的(compact)拓扑空间。将 $\mathbb{Z}$ 视作离散拓扑空间(即一切子集都是开(闭)的)，对每一个 $M\in$ f. g. $\mathrm{P}_R\mathfrak{M}$，定义一个映射(称为**秩函数**(rank function))

$$rk_M:\ \mathrm{Spec}R\to\mathbb{Z};\quad P\longmapsto \mathrm{rank}_P M$$

可得如下结果：

引理 4.4　设 $R\in\mathcal{C}$Ring，$M\in$ f. g. $\mathrm{P}_R\mathfrak{M}$，则对 Spec$R$ 的 Zariski 拓扑与 $\mathbb{Z}$ 的离散拓扑，秩函数 rk_M 是连续的，因此是有界的。

证　不失一般性可令 $M\oplus M'=R^m$，于是由 §2 知 M,M' 各对应 $R^{m\times m}$ 中的幂等矩阵 $e,I-e$(I 为 $m\times m$ 单位矩阵)。

$\forall P\in\mathrm{Spec}R,rk_M(P)=n$ 即 $\mathrm{rank}_P M=n$。由引理 4.3 知这等价于 e 在 $(R/P)^{m\times m}$ 中的象 $\bar{e}$ 有秩 n，于是 $\mathrm{rank}_P M\leqslant n\Leftrightarrow e$ 的一切 $(n+1)\times(n+1)$ 子矩阵的行列式生成的理想 $A\subseteq P$。由此知

$$\{P\in\mathrm{Spec}R\mid \mathrm{rank}_P M\leqslant n\}=\{P\in\mathrm{Spec}R\mid P\supseteq A\}=V(A)$$

为 Spec$R$ 的闭集，但 $\mathrm{rank}\bar{e}\geqslant n\Leftrightarrow\mathrm{rank}(\bar{I}-\bar{e})\leqslant m-n$。因此

$$\{P\in\mathrm{Spec}R\mid \mathrm{rank}_P M\geqslant n\}\text{ 也是闭集。}$$

故

$$rk_M^{-1}(n)=V(A)\cap V(A')$$

为闭集。其中 A' 为 $I-e$ 的一切 $(m-n+1)\times(m-n+1)$ 阶子矩阵的行列式生成的 R 的理想。又显然有 $V(A)=D(A'),V(A')=D(A)$，而 $\{n\}$ 为 $\mathbb{Z}$ 的开集基，故 rk_M 是连续的。

由 Spec$R$ 的紧致性知 rk_M 有界。　□

引理 4.5　设 $R\in\mathcal{C}$Ring，则 R 为连通环(即幂等元只有 0,1 两个)$\Leftrightarrow$ Spec$R$ 为连通的拓扑空间。

证　$\Rightarrow$：反设 Spec$R$ 不连通，则有 Spec$R$ 的非空开集 X_1,X_2 使

$$\mathrm{Spec}R=X_1\dot{\cup}X_2$$

由 X_j 为开集知必有 $A_j\lhd R$ 使 $X_j=D(A_j),j=1,2$。而由 $\mathrm{Spec}R=X_1\cup X_2$ 知 $A_1+A_2=R$。若有 $0\neq x\in A_1\cap A_2$，则 $\forall P\in\mathrm{Spec}R,x\notin P$，即 $x\in R^*$ 于是 $A_1=R$，由此知 $X_1=\mathrm{Spec}R$，于是 $X_2=\varnothing$ 这与上设矛盾，故 $A_1\cap A_2=0$，由此知 $R=A_1\oplus A_2,A_j\neq 0,R$。注意由此知 $1=e+(1-e),e\in A_1,1-e\in A_2$，且 $0,1\neq e=e^2$ 与 R 连通矛盾，因此 Spec$R$ 当 R 连通时必连通。

$\Leftarrow$ 反设 R 不连通，即有 $0,1\neq e=e^2\in R$，由 $0=e(1-e)\in P,\forall P\in S_1$ 知 $e\in P$ 或 $1-e\in P$，但不能都在 P 中(否则 $1=e+(1-e)\in P$，与 P 为素理

想矛盾)。故 $D(e)\neq\varnothing$,$D(1-e)\neq\varnothing$ 且

$$\mathrm{Spec}R = D(e)\ \dot{\bigcup}\ D(1-e)$$

这与 Spec$R$ 连通矛盾,故 Spec$R$ 连通时 R 必连通。 □

注意到 Spec$R$ 连通时,由引理 4.4 知,$\forall M\in \mathrm{f.g.P}_R\mathfrak{M}$,$rk_M:\mathrm{Spec}R\to\mathbb{Z}$ 只能取常值。反过来,若 Spec$R$ 不连通,可设 $R=Re\oplus R(1-e)$,此时,$Re\in \mathrm{f.g.P}_R\mathfrak{M}$ 显然无常数秩。故有:

命题 4.9 设 $R\in\mathcal{C}\mathrm{Ring}$,则 R 为连通环 $\Leftrightarrow \forall M\in \mathrm{f.g.P}_R\mathfrak{M}$,$M$ 都有常数秩,因此整环与交换的局部环都是连通环。

注① 常数秩相同的有限生成投射模未必是稳定同构的,不能由上命题得到"(交换的)连通环的 K_0 群同构于 $\mathbb{Z}$"的结论。读者可想一下:为什么?或参看下面的注②。

应用到半局部环可得:

定理 4.1 设 R 为交换半局部环,则

(1) 若 $M\in \mathrm{f.g.P}_R\mathfrak{M}$ 有常数秩 n,即 $\mathrm{rank}M=n$,则 $M\simeq R^n$($_R\mathfrak{M}$ 中);

(2) 下述三点等价:(a) R 连通;(b) $R\in\mathrm{PF}$,即 $\mathrm{f.g.P}_R\mathfrak{M}=\mathrm{f.g.Free}_R\mathfrak{M}$;(c) $K_0(R)\simeq\mathbb{Z}$(也是环同构)。

证 (1) 设 $\mathrm{Max}R=\{\mathfrak{m}_1,\cdots,\mathfrak{m}_r\}$(注意半局部环极大理想数必定有限),由 $\mathrm{rank}M=n$ 知,可令 $m_{i_1},m_{i_2},\cdots,m_{i_n}\in M$ 在 $M_{\mathfrak{m}_i}$ 中对应的元素为 $M_{\mathfrak{m}_i}$ 的基,$i=1,2,\cdots,r$。由中国剩余定理(推广形式)知,必有 $m_j\in M$ 使

$$m_j\equiv m_{ij}\ (\mathrm{mod}\ \mathfrak{m}_iM),\qquad i=1,2,\cdots,r;\ j=1,2,\cdots,n$$

(注意 $\forall i\neq j$,$\mathfrak{m}_iM+\mathfrak{m}_jM=M$)。因此 $m_1,m_2,\cdots,m_n$ 在 $M_{\mathfrak{m}_i}$ 中对应的元素为 $M_{\mathfrak{m}_i}$ 之基。$i=1,\cdots,r$,记 $e_j=(0,\cdots,0,1,0,\cdots,0)$,$j=1,2,\cdots,n$,为 R^n 的标准正交基,则有 $_R\mathfrak{M}$ 同态

$$f:R^n\to M$$

$$e_j\longmapsto m_j,\quad j=1,2,\cdots,n$$

由此知 $f_{\mathfrak{m}_i}$ 为 $R_{\mathfrak{m}_i}$-模同构,$i=1,2,\cdots,r$。下面来证 f 为 $_R\mathfrak{M}$ 同构,为此先证

(i) $\mathscr{F}=\bigoplus\limits_{\mathfrak{m}\in\mathrm{Max}R}R_{\mathfrak{M}}$ 为忠实平坦的 R-模(即 $\mathscr{F}\in\mathrm{Flat}_R\mathfrak{M}$,且对一切非零 R-模 N,$\mathscr{F}\bigotimes\limits_R N\neq 0$)。事实上,命题 4.3 已指出 $R_{\mathfrak{m}}\in\mathrm{Flat}_R\mathfrak{M}$,$\forall\mathfrak{m}\in\mathrm{Spec}R$,因此 $\mathscr{F}\in\mathrm{Flat}_R\mathfrak{M}$。若有 $A\in{}_R\mathfrak{M}$ 使 $\mathscr{F}\bigotimes\limits_R A=0$,任取 $a\in A$,则 a 在 R 中的零化子 $Ann_R(a)\cap R\backslash\mathfrak{m}\neq\varnothing$,$\forall\mathfrak{m}\in\mathrm{Max}R$(注意 $\mathscr{F}\bigotimes\limits_R A=\bigoplus\limits_{\mathfrak{m}\in\mathrm{Max}R}A_{\mathfrak{m}}$)。因此,$Ann_R(a)\not\subset\mathfrak{M}$,$\forall\mathfrak{M}\in\mathrm{Max}R$,由此知 $Ann_R(a)\subset R^*$,$\forall a\in A$,于是 $A=0$。故 $\mathscr{F}$ 为忠实平坦 R-模。

再来证(ii)：${}_R\mathfrak{M}$ 中 $A'\xrightarrow{g}A\xrightarrow{h}A''$ 正合$\Leftrightarrow$在${}_{R_\mathfrak{m}}\mathfrak{M}$ 中 $A'_\mathfrak{m}\xrightarrow{g_\mathfrak{m}}A_\mathfrak{m}\xrightarrow{h_\mathfrak{m}}A''_\mathfrak{m}$ 正合，$\forall\,\mathfrak{m}\in \mathrm{Max}R$。

$\Rightarrow$：由 $R_\mathfrak{m}\in \mathrm{Flat}_R\mathfrak{M}$，与 $R_\mathfrak{m}\otimes_R B\simeq B_\mathfrak{m}$，$\forall\,B\in{}_R\mathfrak{M}$ 即得。

$\Leftarrow$：由上证的(i)即得。

由(ii)即知，${}_R\mathfrak{M}$ 中任意同态 φ 为单的(满的、同构)$\Leftrightarrow\varphi_\mathfrak{m}$ 在${}_{R_\mathfrak{m}}\mathfrak{M}$ 中为单的(满的，同构)，$\forall\,\mathfrak{m}\in \mathrm{Max}R$，故上面的 $f:R^n\to M$ 为${}_R\mathfrak{M}$ 中的同构，即 $M\simeq R^n$。

(2) (a)$\Rightarrow$(b)：R 连通时由命题 4.9 知一切 $M\in \mathrm{f.g.P}_R\mathfrak{M}$ 都有常数秩，再由已证的(1)知 $M\in \mathrm{f.g.Free}_R\mathfrak{M}$，故 $R\in \mathrm{PF}$。

(b)$\Rightarrow$(c)：是显见的，因为对交换环 R，$R\in \mathrm{PSF}\Leftrightarrow K_0(R)\simeq\mathbb{Z}$，而 $\mathrm{PF}\subset\mathrm{PSF}$。

(c)$\Rightarrow$(a)：设 R 不连通，则 R 可表为 $R=R_1\oplus R_2$，R_1、$R_2\in \mathcal{C}\mathrm{Ring}$，由命题 2.6 与定理 3.4 可知

$$\mathbb{Z}\simeq K_0(R)\simeq K_0(R_1)\oplus K_0(R_2)\simeq\mathbb{Z}^2\oplus\widetilde{K}_0(R_1)\oplus\widetilde{K}_0(R_2)$$

由有限生成 Abel 群的结构定理知，这是不可能的，故 R 为连通环。　□

由上面的证明顺便地已得如下结果(不限于交换局部环)：

推论 4.1　设 $R\in \mathcal{C}\mathrm{Ring}$，则

(1) $\bigoplus_{\mathfrak{m}\in \mathrm{Max}R}R_\mathfrak{m}$ 为忠实平坦 R-模；

(2)${}_R\mathfrak{M}$ 中 $A'\xrightarrow{g}A\xrightarrow{h}A''$正合$\Leftrightarrow$在${}_{R_\mathfrak{m}}\mathfrak{M}$ 中 $A'_\mathfrak{m}\xrightarrow{g_\mathfrak{m}}A_\mathfrak{m}\xrightarrow{h_\mathfrak{m}}A''_\mathfrak{m}$ 正合，$\forall\,\mathfrak{m}\in \mathrm{Max}R$；

(3)${}_R\mathfrak{M}$ 中同态 φ 为单的(满的，同构)$\Leftrightarrow\varphi_\mathfrak{m}$ 在${}_{R_\mathfrak{m}}\mathfrak{M}$ 中为单的(满的，同构)，$\forall\,\mathfrak{m}\in \mathrm{Max}R$。

注意，若交换半局部环 R 的极大理想个数为 k(k 当然有限)，由§3 知，$R/J(R)$必为 k 个域的直积，且 R 又必可分解为 n 个连通的半局部环之直积：$R=R_1\oplus\cdots\oplus R_n$(因为 $k<\infty$)，其中 $n\leqslant k$，这里的 n、k 是由 R 确定的，于是由定理 4.1(2)(c)知 $K_0(R)\simeq\mathbb{Z}^n$。由此可知 $n=k\Leftrightarrow R_j$ 都是局部环，再注意，局部环必为半完全环，而(交换的)连通半完全环必为局部环。事实上，若 S 为(交换的)连通半完全环，则 $S/J(S)$(域的直积)必为域(否则由幂等元提升性质知 S 不连通)。所以又可得如下结果：

定理 4.2　设 R 为交换半局部环，则

(1) $R/J(R)$为 k 个域的直积，其中 k 为 R 的极大理想个数(必有限)；

(2) R 可分解为 $n\leqslant k$ 个连通的半局部环之直积

$$R = R_1 \oplus \cdots \oplus R_n$$

因此 $K_0(R) \simeq \mathbb{Z}^n$；

(3) $K_0(R) \simeq \mathbb{Z}^k$（即 $n=k$）$\Leftrightarrow$(2)中的 R_j 都是局部环$\Leftrightarrow$(2)中的 R_j 都是半完全环。

定理 4.1 中用 K_0 群表征了交换局部环的连通性，对一般的交换环我们可得如下结果（见[Tong,1994]）：

命题 4.10 设 $R \in$ CRing，且 $K_0(R)$ 中无同构于 $\mathbb{Z}^2$ 的直和项（比如当 $\widetilde{K}_0(R)$ 为挠群时），则 R 为连通环。

证 反设 R 不连通，则必有环分解

$$R \simeq R_1 \oplus R_2, \qquad R_j \in \text{CRing}, j = 1,2$$

由命题 2.6 与定理 3.4 得

$$K_0(R) \simeq \mathbb{Z} \oplus \widetilde{K}_0(R) \simeq \mathbb{Z}^2 \oplus \widetilde{K}_0(R_1) \oplus \widetilde{K}_0(R_2) \qquad (2)$$

这就与 $K_0(R)$ 无同构于 $\mathbb{Z}^2$ 的直和项矛盾。又当 $\widetilde{K}_0(R)$ 为挠群时，由于对同构的 Abel 群 G_1, G_2 必然有 $G_1/T(G_1) \simeq G_2/T(G_2)$，其中 $T(G_i)$ 表 G_i 的挠子群。于是，由设知 $K_0(R)/T(K_0(R))$ 无同构于 $\mathbb{Z}^2$ 的直和项，但(2)右边的 Abel 群模去挠子群后有 $\mathbb{Z}^2$ 作直和项，因此(2)不能成立，即 R 必为连通环。 □

注② 命题 4.10 的逆并不成立，因为由 §3 末段知，$\forall n \geqslant 1$ 都有 Dedekind（整）环 R 使 $\mathbb{Z}^n$ 为 $K_0(R)$ 的直和项，但 R 当然总是连通的。又命题 4.10 不能向 IBN 环推广。事实上，对 §1 例 1，取 $S = F \oplus R$，由 $F \in$ IBN 与[佟文廷，1984]知 $S \in$ IBN，而 $K_0(S) \simeq K_0(F) \oplus K_0(R) \simeq \mathbb{Z} \oplus 0 \simeq \mathbb{Z}$ 无同构于 $\mathbb{Z}^2$ 的直和项，但 S 不是连通的（同时 $K_0(S) \simeq \mathbb{Z}$ 也意味着 $S \in$ IBN）。

注③ 交换局部环显然为连通的半局部环，但连通的交换半局部环未必为局部环，甚至未必为半完全环（局部环当然为半完全环），因此对交换环类，局部环与连通的半完全环都是连通的交换半局部环的真子类。见下页之例自明。值得注意的是：尽管如此，连通的交换半局部环仍具有交换局部环的许多性质，如上面讲的 PF 性，K_0 群，以及一些同调性质等。

注意到紧致 Hausdorff 空间 X 的 K^0 群 $K^0(X)$ 与 X 上实（复）连续函数环 $C(X)$ 的 K_0 群 $K_0(C(X))$ 是同构的（比如见[Blackadar,1986]）。又 $C(X)$ 为连通环当且仅当 X 为连通空间（见[Gillman,1976]）。不论 $K^0(X)$，$K_0(C(X))$ 两个群哪个容易计算，我们都可应用下述推论来考察 X 的连通性。

推论 4.2 设 X 为紧致 Hausdorff 空间，若 $K^0(X)(K_0(C(X)))$ 不含同构于 $\mathbb{Z}^2$ 的直和项，则 X 为连通空间。

在本节最后，我们来改进命题 2.3(连通的 PT 环为 PF 环)，来证反方向的结果。

定理 4.3　设 R 为(交换的)PT 环，则 R 为连通环$\Leftrightarrow R\in$ PF。

证　只需证$\Leftarrow$。事实上，注意 $R\in$ PF 必有 $K_0(R)\simeq\mathbb{Z}$，由命题 4.10 即知 R 为连通环。 □

例 1　$R=\{\frac{m}{n}\in Q\mid(m,n)=1,(n,pq)=1\}$，其中 p、q 为两个不同的素数，显然，R 对数的运算为一个连通的交换环。又可看出

$$\mathrm{Max}R=\{pR,qR\}$$
$$J(R)=pR\cap qR=pqR$$
$$R/J(R)\simeq\mathbb{Z}_p\oplus\mathbb{Z}_q\text{(域的直积)}$$

因此，R 为连通的交换半局部环。但显然 R 不是局部环(极大理想个数不惟一)，也不是半完全环($R/J(R)$ 有不为 0，1 的幂等元，而 R 无，因此商环 $R/J(R)$ 的幂等元不能提升)。

第二章 K_1 群的基础理论

K_1 群与典型群有着密切的关系，环 R 的 K_1 群 $K_1(R)$ 事实上就是一般线性群 $GL(R)$（n 维（阶）一般线性群 $GL_n(R)$ 当 $n\to\infty$ 时的极限）的 Abel 化。本章主要介绍 K_1 群最基本的理论与计算法，在学习本章时，建议读者注意如下的两点：一是作为从环范畴到 Abel 群范畴的函子，K_0 与 K_1 有许多共性，比如：$K_i(R_1\oplus R_2\oplus\cdots\oplus R_n)\simeq K_i(R_1)\oplus K_i(R_2)\oplus\cdots\oplus K_i(R_n)$，$i=0,1$；$K_i(R)\simeq K_i(R^{n\times n})$，$i=0,1$，以及对可裂环同态的一些应用等（在下章中将看到 K_2 也有这些性质），二是对交换环的 K_1 群，初等群、特殊线性群及行列式所起的重要作用。注意到这一点，对后面几节研究非交换环上矩阵的行列式（Dieudonné 行列式）以及广义 Euclid 环、Dieudonné 环等的用意就能有较深的领会。正是通过这些研究，我们将 K_1 群的可计算（可估计）范围逐渐扩大，比如扩大到局部环，乃至半局部环。此外，由于 Dedekind 环在代数数论与代数几何中的重要性，我们将 Dedekind 环的 K_1 群列为专节加以介绍，特别是对于 § 6 中介绍的稳定度概念（在直和消去问题中有重要应用），我们证明了 Dedekind 环的稳定度不超过 2，从而将 Dedekind 环的 K_1 群计算归纳为 2 阶矩阵的计算。特别是对代数数域 F 的代数整元环 O_F，我们证明了 $K_1(O_F)$ 为 O_F^*（O_F 的乘法群，即可逆元（单位元）群）与一个挠群 T 的直和，并指出：H. Bass，J. Milnor 与 J. P. Serre 已证出这个 T 是平凡的，因此 $K_1(O_F)\simeq O_F^*$ 且由 Dirichlet 单位定理可将 O_F^* 写成更精密的形式。

§5 环的 K_1 群(Whitehead 群)

在第一章即§1～§4中我们事实上是将域上线性空间、维数及同构类通过 K_0 函子推广到一般环上的有限生成投射模、秩及稳定同构类，这种推广的程度(稳定的程度)是随环类的不同而不同的，K_0 群就是对于这种稳定程度的一个度量。本节中，我们构作 K_1 函子以推广域上线性空间的自同构及其不变量——行列式等，我们将会看到 K_1 群也度量着这种推广的稳定程度(相差的程度)。

设 F 为任一域，则 F 有乘法群 $F^{\cdot}=F\backslash 0$，F 上 n 维线性空间 F^n 的自同构群即 $GL_n(F)$(即使 F 为一般环时，也常称之为 n 维(阶)**一般线性群**(general linear group))。行列式事实上是这两个乘法群之间的满同态

$$det:GL_n(F)\twoheadrightarrow F^{\cdot}$$

其核为

$$\text{Ker det}=SL_n(F)\lhd GL_n(F)$$

其中 $SL_n(F)=\{A\in GL_n(F)\mid detA=1\}$ 称为 F 上的 n 阶(维)**特殊线性群**(special linear group)。记 $E_n(F)$ 为 F 上的 n 阶(维)**初等群**(elementary group)，它是由对角元全为 1，非对角元最多有一个非零的 F 元素的 n 阶矩阵(**初等矩阵**)生成的 $GL_n(F)$ 与 $SL_n(F)$ 的子群。这里不规定对角元最多有一个元素为 F 中的非零元其余对角元全为 1 的对角矩阵为初等矩阵，主要因为这样已能保证 $SL_n(F)=E_n(F)$，再添上这种矩阵则生成 $GL_n(F)$，意义不大，见后面定理 5.2 之证。而且在向环 R 上推广时这种对角阵未必为 $GL_n(R)$ 中元素(R 中非零元未必可逆)，因此下面的 $E_n(R)$ 均指(注意今后 e_{ij}^a 右上肩的 a 不表示方指数!)

$$E_n(R)=\langle\{\begin{pmatrix}1 & & \\ & \ddots & a \\ & & 1\end{pmatrix}=I_n+aE_{ij}\equiv e_{ij}^a\mid a\in R,\ i\neq j\}\rangle$$

即 $\{I_n+aE_{ij}\mid i\neq j, a\in R\}$ 生成的乘法群，称为 R 上 n 阶**初等群(初等矩阵群)**，其中 I_n 为 n 阶单位矩阵，E_{ij} 表示(i,j)位置为 1，其余元素为 0 的 n 阶矩阵。本书中，初等矩阵均指 e_{ij}^a 形的矩阵，e_{ij}^a 左(右)乘某一矩阵对应的变换称为**初等行(列)变换**，而 $GL_n(R)$ 为 R 上 n 阶一般线性群(可逆矩阵群)。当 R∈CRing 时因为可如域的情况一样定义行列式，且 $A\in R^{n\times n}$ 可逆等价于

$\det A\in R^{\cdot}$，$SL_n(R)$可照域的情况同样定义，也称为 R 上的**特殊线性群**。但对非交换环，域上矩阵行列式定义不能照搬，否则将会导致平庸化。比如 R 为除环但非域时，必有 $0\neq a,b\in R$，使 $ab-ba\neq 0$，从而 $ab-ba\in R^{\cdot}$，对 $A\in R^{n\times n}$，先从第 1 行提出因子 a，再从第二行提出因子 b，则 $A=abA_1$，$A_1\in R^{n\times n}$，若先提 b 因子，再提 a 因子，则导致

$$(ab-ba)\det A_1 = 0$$

因此 $\det A_1=0$，于是 $\det A=0$，$\forall A\in R^{n\times n}$，这就形成了推广工作的第一个困难。另外对一般的环 R，R 即使是交换环，也未必有 $E_n(R)\lhd GL_n(R)$（见下例），又造成推广工作的另一困难。

例 1　设 F 为域，$R=F[x,y]$，

$$M=\begin{pmatrix}1+xy & x^2\\ -y^2 & 1-xy\end{pmatrix}。$$

由 $\det M=1$ 知，$M\in SL_2(R)\subset GL_2(R)$，取 $e_{12}^1=\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}\in E_2(R)$，则

$$\begin{aligned}Me_{12}^1M^{-1} &= \begin{pmatrix}1+xy & x^2\\ -y^2 & 1-xy\end{pmatrix}\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}\begin{pmatrix}1-xy & -x^2\\ y^2 & 1+xy\end{pmatrix}\\ &= \begin{pmatrix}1+y^2+xy^3 & 1+2xy+x^2y^2\\ -y^4 & 1-y^2-xy^3\end{pmatrix}\end{aligned}$$

其第 2 行元素都是 4 次多项式，且容易看出

$$\deg(u(-y^4)+v(1-y^2-xy^3)) = 4,$$
$$\forall u,v\in F \text{ 但 } u,v \text{ 不全为 } 0。$$

因此 $Me_{12}^1M^{-1}$不能经右乘任何 $N\in E_2(R)$成为（考虑常数项）：

$$\begin{pmatrix}a & 0\\ 0 & b\end{pmatrix} \quad 或 \quad \begin{pmatrix}0 & a\\ b & 0\end{pmatrix}型, \qquad a,b\in R$$

（注意 N 的每一列中的二元素不可能都不含常数项，否则，$x=y=0$ 时 $\det N\neq 1$）。由此知 $Me_{12}^1M^{-1}\notin E_2(R)$，于是 $E_2(R)$不是 $GL_2(R)$的正规子群。注意到 $\det M=1$，这也更进一步说明了 $E_2(R)$甚至不是 $SL_2(R)$的正规子群。

一般线性群及它的一些特殊子群，如特殊线性群、初等（矩阵）群、辛（矩阵）群、正交（矩阵）群与酉（矩阵）群，统称为矩阵群，也称为**典型群**（classical group），数环（整数环与代数整数（元）环）上的典型群又称为**算术群**。二十世纪四十年代华罗庚最先将域上的典型群理论向数环开拓，五十年代开始已有不少环上典型群的工作，八十年代对交换环上典型群的正规子群问题，因研究典型群单性的需要，在不少人的努力下取得了许多优美而彻底的结

果。在这些工作中,初等群因更易计算与掌握,起了举足轻重的作用。在研究 $GL_n(R)$ 与 $E_n(R)$ 的中间群 G 时,常将 $E_n(R)$ 的性质提升到 G,从而得到 G 的一些性质。$E_n(R)\lhd GL_n(R)$ 时当然使 $E_n(R)\lhd G$,此时对 G 中矩阵 A 作行、列初等变换所得结果可只用行(列)初等变换同样得到,这是因为左陪集 $AE_n(R)$ 与右陪集 $E_n(R)A$ 相等的缘故,因此研究 $E_n(R)$ 在 $GL_n(R)$ 中的正规性十分重要。上述的例 1 是 1966 年由 P. M. Cohn 提供的,1977 年 A. A. Suslin(Суслин)成功地证明了:若 R 为交换环,$n\geqslant 3$,则 $E_n(R)\lhd GL_n(R)$,从而对交换环上的这一问题得到完善的解决,但对非交换环,此结果是否成立,仍未解决。交换环上之所以会出现 Cohn 的反例,主要是因为 $n=2$ 太小,"回旋"余地少(运算限制的范围小),因此在代数 K-理论的研究中采用与§2 平行的方法,即将 $GL_n(R)$ 中的矩阵 A 看作是 $\begin{pmatrix} A & \\ & 1\end{pmatrix}$(末行、末列除对角元 1 之外全为 0,相当于将 R^n 的自同构视作 R^{n+1} 上的自同构)。于是有

$$GL_2(R)\subset GL_3(R)\subset\cdots\subset GL_n(R)\subset GL_{n+1}(R)\subset\cdots$$

记

$$GL(R)=\bigcup_{n\to\infty} GL_n(R)$$

称为 R 上的**一般线性群**。同样地处理 $SL_n(R)$,$E_n(R)$,分别称

$$SL(R)=\bigcup_{n\to\infty} SL_n(R),$$

$$E(R)=\bigcup_{n\to\infty} E_n(R)$$

为 R 上的**特殊线性群、初等群**。显然 $E(R)<SL(R)<GL(R)$,若能证明 $E(R)\lhd GL(R)$,则得 $E(R)\lhd SL(R)$。注意到对任一群 G,换位子(形如 $aba^{-1}b^{-1}$ 的元素)生成的子群 $[G,G]\lhd G$(可直接验证或见后面命题 5.2 之证),于是,我们只需通过一些引理证明 $E(R)=[GL(R),GL(R)]$ 即得 $E(R)\lhd GL(R)$。

引理 5.1 设 $R\in$ CRing,$A\in GL_n(R)$,则有表示式 $A=SD$,其中 $S\in SL_n(R)$,$D=\mathrm{diag}(d,1,\cdots,1)$(对角元为 $d,1,\cdots,1$ 的对角阵),而 $d=\det A$。

证 令 $d=\det A$,由 $A\in GL_n(R)$ 知 $d\in R^{\cdot}$,即 $d^{-1}\in R$。于是令

$$S=A\cdot\mathrm{diag}(d^{-1},1,\cdots,1)=A(\mathrm{diag}(d,1,\cdots,1))^{-1},$$

$$D=\mathrm{diag}(d,1,\cdots,1)$$

则 $S\in SL_n(R)$ 且 $A=SD$。 □

引理 5.2 设 $R\in$ Ring,则在 $R^{n\times n}$ 中

(1) $E_{ij}E_{kl}=\delta_{jk}E_{il}$,因此 $(E_{ij})^2=0$,$\forall i\neq j,k\neq l$;

(2) $e_{ij}^a e_{ij}^b = e_{ij}^{a+b}$，因此$(e_{ij}^a)^{-1} = e_{ij}^{-a}$， $\forall i \neq j, a, b \in R$；

(3) $[e_{ij}^a, e_{jk}^b] = e_{ik}^{ab}$， $\forall i, j, k$ 互异；

(4) $[e_{ij}^a, e_{kl}^b] = I_n$， $\forall j \neq k, i \neq l, i \neq j, k \neq l$，((2),(3)合起来即$[e_{ij}^a, e_{kl}^b] = e_{il}^{\delta_{jk}ab}$)；

(5) $(e_{ij}^a)^T = e_{ji}^a$(T 表转置)。

证 (1)是显见的。由(1)通过$e_{ij}^a = I_n + aE_{ij}$可直接验证(2),(3),(4),(5)。比如以(2)之证为例：

$$
\begin{aligned}
e_{ij}^a e_{ij}^b &= (I_n + aE_{ij})(I_n + bE_{ij}) = I_n + (a+b)E_{ij} + ab(E_{ij})^2 \\
&= I_n + (a+b)E_{ij} = e_{ij}^{a+b}
\end{aligned}
$$
□

引理 5.3 设 $R \in$ Ring，则

$$\mathrm{E}_n(R) < \mathrm{SL}_n(R) \lhd \mathrm{GL}_n(R)$$

证 $\forall E \in \mathrm{E}_n(R)$，则 $\det E = 1$，因此 $\mathrm{E}_n(R) < \mathrm{SL}_n(R)$。

再注意 det 给出群(满)同态 $\det: \mathrm{GL}_n(R) \to R^{\cdot}$，而 $\mathrm{Ker}\det = \mathrm{SL}_n(R)$，即知 $\mathrm{SL}_n(R) \lhd \mathrm{GL}_n(R)$。 □

命题 5.1 设 $R \in$ Ring，$n \geqslant 3$，则 $\mathrm{E}_n(R) = [\mathrm{E}_n(R), \mathrm{E}_n(R)] \subseteq [\mathrm{GL}_n(R), \mathrm{GL}_n(R)]$，因此

$$\mathrm{E}(R) = [\mathrm{E}(R), \mathrm{E}(R)] \subseteq [\mathrm{GL}(R), \mathrm{GL}(R)]$$

证 由 $n \geqslant 3$ 知必有 $1 \leqslant i, j, k \leqslant n$，$i, j, k$ 互异，由引理 5.2(3)得

$$[e_{ij}^a, e_{jk}^1] = e_{ik}^a$$

因此 $\mathrm{E}_n(R) \subseteq [\mathrm{E}_n(R), \mathrm{E}_n(R)]$，注意反向包含是当然的，即得证。 □

引理 5.4 设 $R \in$ Ring，则 $R^{n \times n}$ 中对角元全为 1 的上(下)三角矩阵都在 $E_n(R)$中。

证 注意对角元全为 1 的上(下)三角矩阵都可经 $\hat{j} - a\hat{i}$ 形的一些初等列变换(相当于右乘一些 e_{ij}^{-a}形的初等矩阵)化为 I_n，即得证。 □

引理 5.5 设 $R \in$ Ring，$A, B \in \mathrm{GL}_n(R)$，则

$$\begin{pmatrix} A & \\ & A^{-1} \end{pmatrix}, \begin{pmatrix} [A, B] & \\ & I_n \end{pmatrix} \in \mathrm{E}_{2n}(R),$$

因此

$$\begin{pmatrix} [\mathrm{GL}_n(R), \mathrm{GL}_n(R)] & \\ & I_n \end{pmatrix} \subset \mathrm{E}_{2n}(R)$$

其中分块矩阵中未标示的矩阵块都是 0。

证 用 I 表示 I_n，用分块矩阵的初等变换，则有

$$\begin{pmatrix} A & \\ & A^{-1}\end{pmatrix} \xrightarrow[\hat{2}+\hat{1}]{} \begin{pmatrix} A & A \\ & A^{-1}\end{pmatrix} \xrightarrow[\hat{1}-\hat{2}]{} \begin{pmatrix} & A\\ -A^{-1} & A^{-1}\end{pmatrix}\xrightarrow[\hat{2}+\hat{1}]{}$$

$$\begin{pmatrix} & A \\ -A^{-1} & \end{pmatrix} \xrightarrow[\hat{2}-A\hat{1}]{} \begin{pmatrix} & A\\ -A^{-1} & I\end{pmatrix}\xrightarrow[\hat{1}+A^{-1}\hat{2}]{}\begin{pmatrix} I & A\\ & I\end{pmatrix}\in \mathrm{E}_{2n}(R)\text{（引理 5.4）。}$$

由此知

$$\begin{aligned}&\begin{pmatrix} A & \\ & A^{-1}\end{pmatrix}\begin{pmatrix} I & I\\ & I\end{pmatrix}\begin{pmatrix} I & \\ -I & I\end{pmatrix}\begin{pmatrix} I & I\\ & I\end{pmatrix}\begin{pmatrix} I & -A\\ & I\end{pmatrix}\begin{pmatrix} I & \\ A^{-1} & I\end{pmatrix}\\ &=\begin{pmatrix} I & A\\ & I\end{pmatrix}\in \mathrm{E}_{2n}(R)\text{（引理 5.4）}\end{aligned}$$

因此

$$\begin{pmatrix} A & \\ & A^{-1}\end{pmatrix}\in \mathrm{E}_{2n}(R),\quad \begin{pmatrix} A^{-1} & \\ & A\end{pmatrix}=\begin{pmatrix} A^{-1} & \\ & (A^{-1})^{-1}\end{pmatrix}\in \mathrm{E}_{2n}(R),$$

$$\begin{aligned}\begin{pmatrix} [A,B] & \\ & I\end{pmatrix}&=\begin{pmatrix} ABA^{-1}B^{-1} & \\ & A^{-1}B^{-1}BA\end{pmatrix}\\ &=\begin{pmatrix} A & \\ & A^{-1}\end{pmatrix}\begin{pmatrix} B & \\ & B^{-1}\end{pmatrix}\begin{pmatrix} A^{-1}B^{-1} & \\ & (A^{-1}B^{-1})^{-1}\end{pmatrix}\in \mathrm{E}_{2n}(R)\end{aligned}\qquad\square$$

由上面初等列变换的前三步已可看出

$$(\cdots\ \hat{i}\ \cdots\ \hat{j}\ )\xrightarrow[\hat{j}+\hat{i},\ \hat{i}-\hat{j},\ \hat{j}+\hat{i}]{}(\cdots -\hat{j}\ \cdots\ \hat{i}\ \cdots)$$

对行变换也有类似结果。因此对角矩阵（分块对角矩阵）对角元（对角块）的交换（或排列）相当于左、右乘一些初等矩阵。由此立得：

推论 5.1　设 $R\in$ Ring，则

(1) $$\begin{aligned}&\begin{pmatrix} [\mathrm{GL}_n(R),\mathrm{GL}_n(R)] & \\ & I_n\end{pmatrix}\cup\begin{pmatrix} I_n & \\ & [\mathrm{GL}_n(R),\mathrm{GL}_n(R)]\end{pmatrix}\\ &\subset\begin{pmatrix} [\mathrm{GL}_n(R),\mathrm{GL}_n(R)] & \\ & [\mathrm{GL}_n(R),\mathrm{GL}_n(R)]\end{pmatrix}\\ &\subset \mathrm{E}_{2n}(R);\end{aligned}$$

(2) 若 A 为对角矩阵（分块对角矩阵），其对角线上除 1（单位矩阵）之外为有限对互逆元（互逆矩阵）或为有限个 $\mathrm{GL}_n(R)$ 中的换位子，（n 可为 1），则 $A\in \mathrm{E}(R)$。特别地，$\mathrm{diag}(1,\cdots,1,a^{-1},a,1,\cdots,1,\cdots)\in \mathrm{E}(R)$；

(3) $\begin{pmatrix} & A\\ -A^{-1} & \end{pmatrix}\in \mathrm{E}_{2n}(R)$，$\forall A\in \mathrm{GL}_n(R)$。特别地，$\begin{pmatrix} & 1\\ -1 & \end{pmatrix}$，

$\begin{pmatrix} & -1 \\ 1 & \end{pmatrix} \in E_2(R)$。

现在不难证明定义 K_1 群的关键性结果。

命题 5.2(Whitehead **引理**) 设 $R\in\mathcal{R}$ing,则

$$E(R) = [GL(R), GL(R)] = [E(R), E(R)]$$

因此 $E(R) \lhd GL(R)$ 且 $E(R)$ 为**完全群**(perfect group)($G=[G,G]$时称 G 为**完全群**)。

证 由引理 5.5 令 $n\to\infty$即得

$$[GL(R), GL(R)] \subseteq E(R)$$

但由命题 5.1 知

$$E(R) = [E(R), E(R)] \subseteq [GL(R), GL(R)]$$

因此

$$E(R) = [GL(R), GL(R)] = [E(R), E(R)]$$

下面只需证 $\forall A\in GL(R), A[GL(R), GL(R)]=[GL(R), GL(R)]A$. 事实上,任取 $B, C\in GL(R)$,则由

$$ABCB^{-1}C^{-1} = (ABA^{-1})(ACA^{-1})(AB^{-1}A^{-1})(AC^{-1}A^{-1})A$$

即知。 □

由命题 5.2 即可对任意环定义 K_1 群。

定义 5.1 设 $R\in\mathcal{R}$ing,记

$$\begin{aligned} K_1(R) &= GL(R)/E(R) = GL(R)/[GL(R), GL(R)] \\ &= GL(R)^{ab} \ (GL(R) \text{ 的 Abel 化}) \end{aligned}$$

称 $K_1(R)$为环 R 的 K_1 **群**(**也称为** R **的 Whitehead 群**)。

由此定义知,$K_1(R)$即 $GL(R)$的 Abel 化,因此为 Abel 群。$K_1(R)$的元素 $\bar{A}=A(\bmod E(R))$可看作是 A 的"广义"行列式,(有时称为 **Whitehead 行列式**)。因此 K_1 群非直接地但却本质地推广着域及交换环上可逆矩阵的行列式(在初等变换下不变!)的属性。对任意群 G 的整群环$\mathbb{Z}G$,$\pm g$ $(g\in G)$可看作是$\pm g\in GL_1(\mathbb{Z}G)\subset GL(\mathbb{Z}G)$,将它们对应于 $K_1(\mathbb{Z}G)$的元素生成的子群记为$\pm G$,则称 $Wh(G)=K_1(\mathbb{Z}G)/\pm G$ 为 **G 的 Whitehead 群**。这方面已有内容丰富的专著[Oliver,1988]。

注意对任意环同态 $f:R\to S$ 诱导出(标准的)群同态 $GL(f):GL(R)\to GL(S)$。因此也诱导出 Abel 群同态 $GL^{ab}(f):GL(R)^{ab}\to GL(S)^{ab}$,即诱导出 K_1 群间的同态

$$K_1(f): K_1(R) \to K_1(S)$$

经常规且显见的验证即得:

定理 5.1　K_1: Ring→AG 为一个共变函子。

对于任意域,我们容易证明下述结果:

定理 5.2　设 F 为任意域,则 $K_1(F)\simeq F^{\cdot}$ 且 $SL_n(F)=E_n(F)$, $\forall n\geqslant 2$, 因此 $SL(F)=E(F)$。

证　由引理 5.1,令 $n\to\infty$ 知,$\forall A\in GL(F)$, $A=SD$,其中 $S\in SL(F)$, $D=\mathrm{diag}(\det A,1,1,\cdots)$,记

$$D(F)=\begin{pmatrix} F^{\cdot} & & & & \\ & 1 & & & \\ & & \ddots & & \\ & & & 1 & \\ & & & & \ddots \end{pmatrix}$$

则有 $GL(F)=SL(F)D(F)$。显然 $D(F)$ 与 $F^{\cdot}$ 是同构的乘法群,因此只需再证 $SL(F)=E(F)$ 即可,这显然只要证明 $SL_n(F)\subseteq E_n(F)$ 即可。

事实上任取 $S=(s_{ij})_{n\times n}\in SL_n(F)$, S 的第 1 列当然不全为 0,可令 $s_{11}\neq 0$(否则必有 $s_{i1}\neq 0$ 经(1)+(i)(相当于 S 左乘初等矩阵 e_{1i}^{1}),即使(1,1)位置不为 0)。作行变换(i)$-s_{i1}s_{11}^{-1}$(1), $\forall i\neq 1$,将第 1 列(1,1)以外位置的元素都变为 0,即有 $T_1\in E_n(F)$ 使

$$T_1S=\begin{pmatrix} s_{11} & * \\ & S_1 \end{pmatrix}\quad (*\text{ 处可不为 }0,\text{空处为 }0)$$

于是 $1=\det S=s_{11}\det S_1$,用归纳法知必有 $T_2\in E_n(F)$ 使

$$T_2T_1S=\begin{pmatrix} s_{11} & & & * \\ & s'_{22} & & \\ & & \ddots & \\ & & & s'_{nn} \end{pmatrix}\text{且 } s_{11}s'_{22}\cdots s'_{nn}=1$$

同理再用行变换(i)$-s'_{in}s'^{-1}_{nn}$(n) $i\neq n$ 等仿上知,有 $T_3\in E_n(F)$ 使

$$T_3T_2T_1S=\mathrm{diag}(s''_{11},s''_{22},\cdots,s''_{n-1,n-1},s'_{nn})\text{ 且 } s''_{11}s''_{22}\cdots s''_{n-1,n-1}s'_{nn}=1。$$

最后记 $t_1=\mathrm{diag}(s''^{-1}_{11},s''_{11},1,\cdots,1)$, $t_2=\mathrm{diag}(1,(s''_{11}s''_{22})^{-1},s''_{11}s''_{22},1,\cdots,1)$, $\cdots$, $t_{n-1}=\mathrm{diag}(1,\cdots,1,(s''_{11}\cdots s''_{n-1,n-1})^{-1},s''_{11}\cdots s''_{n-1,n-1})$,则由推论 5.1(2)知 $t_j\in E_n(F)$, $j=1,\cdots,n-1$,而容易看出

$$t_{n-1}t_{n-2}\cdots t_1T_3T_2T_1S=I_n$$

因此 $S\in E_n(F)$ 即 $SL_n(F)\subseteq E_n(F)$,这就说明了 $SL_n(F)=E_n(F)$。　□

用上面的证法可得(注意 R 不是交换环时 $d_j\in R$ 使 $d_1\cdots d_n=1$ 不能保证 d_j^{-1} 都存在, $j=1,\cdots,n$)。

推论 5.2 设 $R\in$ Ring,

(1) 若 $d_1,d_2,\cdots,d_n\in R$ 使 $d_1d_2\cdots d_n=1$,且 n 阶对角矩阵 $D=\text{diag}(d_1,d_2,\cdots,d_n)\in \text{GL}_n(R)$,则 $D\in \text{E}_n(R)$;

(2) 若 $B\in R^{n\times n}$为对角元素可逆的上(下)三角矩阵且对角元之积为 1,则 $B\in \text{E}_n(R)$。

注意,定理 5.2 事实上可表为:设 F 为域,则

$$\text{K}_1(F)\simeq F^{\cdot}\oplus \text{SL}(F)/\text{E}(F)$$

下面我们试着将此结果向交换环推广,来证明下述结果(此结果在形式上平行于定理 3.4 中 K_0 群的分解:$\text{K}_0(R)\simeq \mathbb{Z}\oplus\widetilde{\text{K}}_0(R)$)。

定理 5.3 设 $R\in$ CRing,则

$$\text{K}_1(R)\simeq R^{\cdot}\oplus \text{SL}(R)/\text{E}(R)$$

证 对群同态正合列

$$1\to \text{SL}_n(R)\to \text{GL}_n(R)\xrightarrow{\det} R^{\cdot}\to 1$$

令 $n\to\infty$得群同态正合列

$$1\to \text{SL}(R)\to \text{GL}(R)\xrightarrow{\det} R^{\cdot}\to 1$$

注意由 $\text{E}(R)\lhd \text{GL}(R)$可知 $\text{E}(R)\lhd \text{SL}(R)$;由 $\text{K}_1(R)=\text{GL}(R)/\text{E}(R)\in$ AG 知 $\text{SL}(R)/\text{E}(R)\in$ AG。记$\overline{\det}$为 det mod$\text{E}(R)$意义下得到的群同态,则有 AG 正合列

$$1\to \text{SL}(R)/E(R)\to \text{K}_1(R)\xrightarrow{\overline{\det}} R^{\cdot}\to 1$$

对 Abel 乘法群 G,定义 $ng=g^n$,$\forall g\in G,n\in\mathbb{Z}$。则 $G\in {}_{\mathbb{Z}}\mathfrak{M}$,于是上列是${}_{\mathbb{Z}}\mathfrak{M}$正合列。

又群同构

$$R^{\cdot}\simeq \text{diag}(R^{\cdot},1,\cdots,1,\cdots)$$

给出 Abel 群的单同态 $i:R^{\cdot}\to \text{GL}(R)/E(R)=\text{K}_1(R)$使$\overline{\det}\cdot i=I_{R^{\cdot}}$,因此上列为${}_{\mathbb{Z}}\mathfrak{M}$ 中的可裂正合列,故

$$\text{K}_1(R)\simeq R^{\cdot}\oplus \text{SL}(R)/\text{E}(R)$$ □

定义 5.2 设 $R\in$ CRing,记

$$\text{SK}_1(R)=\text{SL}(R)/\text{E}(R)$$

称为 R 的**特殊 K_1 群**(special K_1-group)或**约化 K_1-群**(reduced K_1-group),有时也称为**特殊 Whitehead 群**。

于是定理 5.3 可改写为:

定理 5.3′ 设 $R\in$ CRing,则

$$K_1(R) \simeq R^{\cdot} \oplus SK_1(R)$$

因此当 $SK_1(R)=1$ 即 $SL(R)=E(R)$(比如 R 为域)时,$K_1(R) \simeq R^{\cdot}$。

注① 由定理 5.3′知 $SK_1(R)$度量着 $SL(R)$与 $E(R)$之差距,也即度量着环 R 在这方面的稳定度(指与域的差距),因此也可称 $SK_1(R)$为 R 的**稳定 K_1 群**。对交换环 R 确定 $SL(R)$与 $E(R)$($SL_n(R)$与 $E_n(R)$)是否相等是一个很有意义的课题,这方面的下述结果值得一提(见[McDonald,1984])。

1966 年,P. M. Cohn 给出例子说明在 F 为域,$m \geqslant 2$ 时可能有 $SL_2(F[x_1,\cdots,x_m]) \neq E_2(F[x_2,\cdots,x_m])$,他还给出一个例子,对 $R=\mathbb{R}[x,y]/(x^2+y^2-1)$(单位圆的坐标环,是 Dedekind 环,事实上,平面代数曲线无奇点(光滑)$\Leftrightarrow$ 它的坐标环为 Dedekind 环),$SL_2(R) \neq E_2(R)$。

1967 年,H. Bass,J. Milnor 与 J. P. Serre 的结果已说明了:当 $n \geqslant 3$,R 为代数数域 F($\mathbb{Q}$ 的有限扩张)的代数整元环 O_F 时,$SL_n(R)=E_n(R)$,因此 $SK_1(O_F)=1$。

1968 年,R. G. Swan 进一步证明了:当 $n \geqslant 3$,R 为 Dedekind 环且商域为代数数域时,$SL_n(R)=E_n(R)$,但 $n=2$ 不真(如 $R=\mathbb{Z}[\sqrt{-5}]$时)。

1974 年,H. Bass 给出一个 $R \in$ PID 使 $SL_2(R) \neq E_2(R)$的例子。

1980 年,F. Ischebeck,1981 年 D. Grayson 都找出使 $SK_1 \neq 1$ 的 PID 例子。(见[Rosenberg,1994])。

1977 年,A. A. Suslin 证明了:设 F 为域,$n \geqslant 3$,则 $SL_n(F[x_1,\cdots,x_n])=E_n(F[x_1,\cdots,x_n])$,同时猜测:$SL_n(F[x_1,\cdots,x_m])=E_n(F[x_1,\cdots,x_m])$,$\forall n \geqslant 3$。

1981 年,T. Vorst 证明了 Suslin 的上述猜测。

1972 年 R. Alperin,R. K. Dennis 与 M. Stein 给出对整群环 $\mathbb{Z}G$,$SK_1(\mathbb{Z}G) \neq 1$ 的第一个例子(见[Oliver,1988]或 LNM,353(1973),1—7),即对 $G \simeq (\mathbb{Z}_p)^n$,$n \geqslant 3$,$p$ 为奇素数。$\mathbb{Z}_p$ 表示 $\mathbb{Z}/p\mathbb{Z}$,$SK_1(\mathbb{Z}G) \neq 1$,且证出 $SK_1(\mathbb{Z}G)=1 \Leftrightarrow G \simeq (\mathbb{Z}_2)^n$ 或 G 的 Sylow 子群都是形如 C_{p^n} 或 $C_{p^n} \times C_p$(其中 C_m 表 m 阶循环群)。

1978 年,B. Magurn 证明了对二面体群(dihedral group)G,$SK_1(\mathbb{Z}G)=1$。(见[Oliver,1988])。

1987 年 V. Srinivas 给出一个正规幺半群 L 使 $SK_1(\mathbb{Z}[L]) \neq 1$。(见[Inassaridze,1990])。

1988 年,J. Gubeladze 证明了:存在秩为 2 的正规幺半群 L(即 $nx \in L \Rightarrow x \in L$,$\forall n \geqslant 1$,$x$ 为 L 之商群的元素)使 $SK_1(\mathbb{Z}[L]) \neq 1$。(见[Inassaridze,1990])。

现在我们给出几个对讨论更复杂环类的 K_1 群有用的结果。

定理 5.4 设 $R_i \in \mathscr{R}$ing, $i=1,\cdots,m$,则

$$K_1(R_1 \oplus \cdots \oplus R_m) \simeq K_1(R_1) \oplus \cdots \oplus K_1(R_m)$$

证 显然有

$$GL_n(R_1 \oplus \cdots \oplus R_m) \simeq GL_n(R_1) \oplus \cdots \oplus GL_n(R_m)$$

令 $n \to \infty$ 则有

$$GL(R_1 \oplus \cdots \oplus R_m) \simeq GL(R_1) \oplus \cdots \oplus GL(R_m)$$

再作 Abel 化即得

$$GL(R_1 \oplus \cdots \oplus R_m)^{ab} \simeq GL(R_1)^{ab} \oplus \cdots \oplus GL(R_m)^{ab}$$

即

$$K_1(R_1 \oplus \cdots \oplus R_m) \simeq K_1(R_1) \oplus \cdots \oplus K_1(R_m) \qquad \square$$

定理 5.5 设 $R \in \mathscr{R}$ing,则

$$K_1(R^{n\times n}) \simeq K_1(R).\ (K_1 \text{ 群的弱 Morita 不变性})。$$

证 注意到 $GL(R^{n\times n}) \subset GL(R)$,经适当分 $n\times n$ 块又知 $GL(R) \subset GL(R^{n\times n})$,于是 $GL(R^{n\times n}) = GL(R)$,作 Abel 化即得证。 □

定理 5.6 设有环同态 $f:R\to S$ 与 $g:S\to R$ 使 $gf=I_R$,则

(1) $K_1(f)$为单同态,因此在同构意义下,$K_1(R)$为 $K_1(S)$的子群,记为 $K_1(R) \lesssim K_1(S)$;

(2) $K_1(g)$为满同态,因此 $K_1(R)$为 $K_1(S)$的商群(同态象);

(3) $K_1(S) \simeq K_1(R) \oplus \mathrm{Ker}\, K_1(g) = \mathrm{Im} K_1(g) \oplus \mathrm{Ker}\, K_1(g)$。

证 同定理 2.5 之证(将 K_0 换为 K_1 即可)。 □

用于多项式环则有:

推论 5.3 $\forall R \in \mathscr{R}$ing,

$$K_1(R[x_1,\cdots,x_m]) \simeq K_1(R) \oplus \mathrm{Ker}\, K_1(g),$$

其中 $g:R[x_1,\cdots,x_n] \to R$ 为使 $g(h(x_1,\cdots,x_n)) = h(0,\cdots,0)$的环同态。

推论 5.4 设 $R \in \mathscr{R}$ing,G 为(乘法)群,则

$$K_1(RG) \simeq K_1(R) \oplus \mathrm{Ker} K_1(g),$$

其中 $g:RG\to R$ 为使 $g(\Sigma r_i g_i) = \Sigma r_i$ 的环同态。

容易验证:$GL, GL_n, E, E_n: \mathscr{R}ing\to \mathscr{G}$(群范畴),$SL, SL_n: \mathscr{C}\mathscr{R}ing\to \mathscr{G}$,及 $SK_1: \mathscr{C}\mathscr{R}ing\to \mathscr{A}\mathscr{G}$ 都是共变函子。再加上一些直接验证可得如下结果:

定理 5.7 对于 $\mathscr{R}$ing,定理 5.4,定理 5.6(1),(2)对 GL, GL_n, E, E_n 仍成立;定理 5.5 对 GL, E 仍成立;定理 5.6(1),(2)对任一共变函子 $F: \mathscr{R}$ing $\to \mathscr{G}$ 都成立;定理 5.6(1),(2),(3),推论 5.3,推论 5.4 对任一共变函子 $F_1: \mathscr{R}$ing$\to \mathscr{A}\mathscr{G} = {}_{\mathbb{Z}}\mathfrak{M}$ 都成立。

定理 5.8　对于 CRing，

(1) 定理 5.4 对 SK_1 成立，即

$$SK_1(R_1 \oplus \cdots \oplus R_m) \simeq SK_1(R_1) \oplus \cdots \oplus SK_1(R_m)$$

且定理 5.4 对 SL_n，E_n，SL，E 也成立；

(2) 定理 5.5 对 SL 仍成立；

(3) 定理 5.6(1)，(2)对 SL，SL_n，SK_1 仍成立；

(4) 定理 5.6(3)，推论 5.3，推论 5.4 对 SK_1 仍成立。

§6　广义 Euclid 环(GE 环)及其 K_1 群

在上节中我们已知道，对任意交换环 R，$K_1(R) \simeq SL(R)/E(R) \oplus R^{\cdot}$，$GL_n(R) = SL_n(R)D_n(R)$，其中 $D_n(R) = \mathrm{diag}(R^{\cdot}, I_{n-1}) \simeq R^{\cdot}$，又由 $SL_n(R) \lhd GL_n(R)$ 用群的第二同构定理可知

$$\begin{aligned} GL_n(R)/SL_n(R) &= SL_n(R)D_n(R)/SL_n(R) \\ &\simeq D_n(R)/SL_n(R) \cap D_n(R) \simeq D_n(R) \simeq R^{\cdot} \end{aligned}$$

从中可看出，研究 $E_n(R)$ 与 $GL_n(R)$ 的中间群对计算 K_1 群是有意义的。由于 $SL_n(R)$ 是由行列式定义的，对一般的非交换环无法照搬，因此本节中我们考察 $E_n(R)$ 与 $GL_n(R)$ 的一种中间群——由 $E_n(R)$ 与可逆 n 阶对角矩阵生成的群。先给出如下定义(事实上，我们又"回到了"线性代数中的"初等矩阵群"，只是将域 F 中 $0 \neq a \in F$ 即 $a \in F^{\cdot}$ 改为 $a \in R^{\cdot}$，允许作 $a(i)$，$a\widehat{j}$ 形的行列变换，因此允许行对调与列对调，见 §5。

定义 6.1　设 $R \in$ Ring，记 $GE_n(R)$ 为 $GL_n(R)$ 中由 $E_n(R)$ 与一切 n 阶可逆对角矩阵生成的子群，(当然有 $E_n(R) < GE_n(R) < GL_n(R)$)，称 $GE_n(R)$ 为 R 上的 n 阶**广义初等矩阵群**。(R 为域时，$GE_n(R)$ 即线性代数中的 n 阶"初等矩阵"群)。

当 $GE_n(R) = GL_n(R)$ 时，称 R 为 **GE_n 环**，记为 $R \in GE_n$；

当 $GE_n(R) = GL_n(R)$ 对无穷多个 n 成立时，称 R 为**稳定 GE 环**，记为 $R \in SGE$；

当 $GE_n(R) = GL_n(R)$ 对一切 n 成立时，称 R 为**广义 Euclid 环**或 **GE 环**，记为 $R \in GE$。

注①　研究使 $E_n(R) = GE_n(R)$ 的环 R 无意义，因为域也不具备这个性质，因此对 K_1 群的研究更无意义。

由定义 6.1 可得：

命题 6.1 在$\mathfrak{R}$ing 中，

(1) $\mathrm{GE} \subset \mathrm{GE}_n \cap \mathrm{SGE}$；

(2) $\mathfrak{R}$ing$=\mathrm{GE}_1$；

(3) $\mathrm{GE}_n(R)=\{A\in \mathrm{GL}_n(R)\,|\,A$ 可经$(i)+a(j)(\hat{k}+b\hat{l})$形行(列)初等变换对角化$\}$；

(4) 域，除环，局部环(未必为交换环)，Euclid 环(未必为交换环)都是 GE 环；

(5) GE_n，SGE，GE 环类都对环的直积封闭。GE 环，SGE 环上的 $m\times m$ 矩阵环仍分别为 GE 环，SGE 环。因此(Artin)半单环为 GE 环。

证 (1)，(2)是显见的。

(3) 由(注意 $De_{ij}^{x}D^{-1}=D(I_n+x\mathrm{E}_{ij})D^{-1}=I_n+D(x\mathrm{E}_{ij})D^{-1}$)

$$\mathrm{diag}(d_1,d_2,\cdots,d_n)e_{ij}^{x} = e_{ij}^{d_i x d_j^{-1}}\,\mathrm{diag}(d_1,d_2,\cdots,d_n) \qquad (*)$$

即得。

由(3)得(5)是显然的。

(4) 只需证局部环，Euclid 环为 GE 环。

(i) 设 R 为局部环，任取 n 与 $A=(a_{ij})\in \mathrm{GL}_n(R)$，则有 $B=(b_{ij})=A^{-1}\in \mathrm{GL}_n(R)$。若 $a_{11},a_{21},\cdots,a_{n1}$都不是 R 中可逆元，则 $a_{j1}\in \mathfrak{m}$(R 惟一的极大理想，对加(减)法封闭)，$j=1,\cdots,n$。于是

$$1=\sum_{j=1}^{n} b_{1j}a_{j1}\in \mathfrak{m}$$

这是不可能的，因此必有 a_{j1} 为 R 中的可逆元。由引理 5.5 后面一段所证同理可知，作(j)与(1)的行对调：$(j)\leftrightarrow(1)$(相当于 A 左乘三个初等矩阵与一个第 j 个对角元为-1，其余对角元为 1 的可逆对角阵)可将 a_{j1} 调到(1,1)位置，因此可设 $a_{11}\in R^{\cdot}$，于是 A 可经初等行列变换将第一行，第一列其余位置化为 0，即有初等矩阵 T_1,T_2 使

$$T_1AT_2=\begin{pmatrix} a_{11} & \\ & A_1 \end{pmatrix}$$

其逆矩阵必为

$$\begin{pmatrix} a_{11}^{-1} & \\ & B_1 \end{pmatrix}$$

形。因此

$$A_1\in \mathrm{GL}_{n-1}(R)$$

故用归纳法即知有初等矩阵 T_3,T_4 使 T_3AT_4 为可逆对角矩阵，由此知 R

$\in GE_n$，$\forall n$，即 $R \in GE$。

(ii) 设 R 为 Euclid 环，对应 Euclid(左或右)除法的映射为

$$\delta: R \backslash 0 \to \mathbb{N}$$

仿上段证明，不失一般地可设 $A=(a_{ij})\in GL_n(R)$ 且

$$\delta(a_{11}) = \min\{\delta(a_{1j}),\delta(a_{j1}),j = 1,\cdots,n\}$$

于是经有限次 Euclid 除法与分别对应 $T_1,T_2 \in E_n(R)$ 的初等行列变换与行(列)对调将 A 化成

$$T_1AT_2 = \begin{pmatrix} c & \\ & A_2 \end{pmatrix}, \qquad c \in R^{\cdot}, A_2 \in GL_{n-1}(R)$$

因此由归纳法即可证得 $A \in GE_n(R)$，从而知 $R \in GE$。 □

注② 由上证知，对(n 阶)矩阵施以行对调(列对调)相当于对此矩阵左(右)乘广义初等矩阵($GE_n(R)$的元素)，对角阵中对角元的对调则相当于左、右乘初等矩阵($E_n(R)$的元素)。

由命题 6.1 与推论 5.2 立得如下结果(域上相应结果的推广)。

推论 6.1 设 $R \in \mathbb{C}\mathrm{Ring}$，且 R 为局部环、Euclid 环或半单 Artin 环，则 $SL_n(R)=E_n(R)$，$\forall n \geqslant 2$，因此 $SL(R)=E(R)$，$K_1(R)\simeq R^{\cdot}$。

我们还可证更一般的结果，为此先证一条引理，该引理用于交换环是 1977 年 A. A. Suslin 一个重要结果($E_n(R) \lhd GL_n(R)$，$\forall n \geqslant 3$，$R \in \mathbb{C}\mathrm{Ring}$)的特例。

引理 6.1 设 $R \in \mathrm{Ring}$，$D=\mathrm{diag}(d_1,d_2,\cdots,d_n)$为可逆对角矩阵，$B \in E_n(R)$，则 $DBD^{-1}\in E_n(R)$，因此，$R \in GE_n$ 时，$E_n(R) \lhd GL_n(R)$，$\forall n \geqslant 2$。

证 令 $B=e_{i_1j_1}^{a_1}\cdots e_{i_rj_r}^{a_r}$，则

$$DBD^{-1} = (De_{i_1j_1}^{a_1}D^{-1})\cdots(De_{i_rj_r}^{a_r}D^{-1})$$

于是由命题 6.1(3)之证中的(*)式得：右端为初等矩阵之积，即 $DBD^{-1}\in E_n(R)$。 □

定理 6.1 设 $R \in \mathbb{C}\mathrm{Ring}$，则

(1) $R \in GE_n \Leftrightarrow SL_n(R)=E_n(R) \lhd GL_n(R)$；

(2) $R \in SGE \Leftrightarrow SK_1(R)=1 \Leftrightarrow K_1(R)\simeq R^{\cdot}$；

(3) $R \in GE \Leftrightarrow E_n(R)=SL_n(R)$，$\forall n \geqslant 1$

$\Leftrightarrow \forall n \geqslant 1$，$GL_n(R)=E_n(R)D_n(R)$

$\Rightarrow SK_1(R)=1$，因此 $K_1(R)\simeq R^{\cdot}$。

证 (1) $\Rightarrow$：由 $R \in GE_n$ 知，$\forall A \in SL_n(R) \subset GL_n(R)$必可表示为如下形式

$$A = B_1 D_1 B_2 D_2 \cdots B_k D_k,$$

其中 $B_j \in \mathrm{E}_n(R)$，D_j 为 n 阶可逆对角阵，它们都可为 I_n，$j=1,\cdots,k$，于是

$$A = B_1(D_1 B_2 D_1^{-1})(D_1 D_2)B_3(D_1 D_2)^{-1})\cdots((D_1 D_2\cdots$$

$$D_{k-1})B_k(D_1 D_2\cdots D_{k-1})^{-1})D_1 D_2\cdots D_k$$

记 $D=D_1 D_2\cdots D_k=\mathrm{diag}(d_1,d_2,\cdots,d_n)$。由引理6.1知

$$B_1(D_1 B_2 D_1^{-1})((D_1 D_2)B_3(D_1 D_2)^{-1})\cdots$$

$$((D_1 D_2\cdots D_{k-1})B_k(D_1 D_2\cdots D_{k-1})^{-1}) \in \mathrm{E}_n(R)$$

而由推论5.2又知 $D\in \mathrm{E}_n(R)$（这是因为 $\det A=\det D=d_1 d_2\cdots d_n=1$）。因此 $A\in \mathrm{E}_n(R)$，即 $\mathrm{SL}_n(R)=\mathrm{E}_n(R)$。

$\Leftarrow$：由引理5.1知，$\forall A\in \mathrm{GL}_n(R)$，$A=SD$，其中 $S\in \mathrm{SL}_n(R)=\mathrm{E}_n(R)$，$D$ 为对角可逆阵，由此即知 $R\in \mathrm{GE}_n$。

(2) 第二个"$\Leftrightarrow$"是已知结果，下证第一个"$\Leftrightarrow$"。

$\Rightarrow$：由(1)知，当 $R\in \mathrm{SGE}$ 时，必有无限多个 n 使 $\mathrm{E}_n(R)=\mathrm{SL}_n(R)$，且 $\mathrm{E}_m(R)\neq \mathrm{SL}_m(R)$ 时必有 $n>m$ 使 $\mathrm{E}_n(R)=\mathrm{SL}_n(R)$，于是

$$\mathrm{SK}_1(R) = \bigcup_{n\to\infty} \mathrm{SL}_n(R)/\bigcup_{n\to\infty} \mathrm{E}_n(R) = 1$$

因此 $\mathrm{K}_1(R)\simeq R^{\cdot}$（由定理5.3）。

$\Leftarrow$：反设 $R\notin \mathrm{SGE}$，即只有限个 n 使 $\mathrm{GE}_n(R)=\mathrm{GL}_n(R)$，于是有 n_0 使 $m\geqslant n_0$ 时，$\mathrm{GE}_m(R)\neq \mathrm{GL}_m(R)$，即 $R\notin \mathrm{GE}_m(R)$，由(1)知当 $m\geqslant n_0$ 时，$\mathrm{SL}_m(R)\neq \mathrm{E}_m(R)$，因此 $\mathrm{SK}_1(R)\neq 1$，与 $\mathrm{SK}_1(R)=1$ 矛盾。

(3) 由(1)，(2)及引理5.1即得。 □

注意到整数环 $\mathbb{Z}$，以及域 F 上的一元多项式环 $F[x]$ 都是Euclid整环，因此为GE环。于是有

例1 $\mathrm{K}_1(\mathbb{Z})=\{\pm 1\}\simeq \mathbb{Z}_2$

$$\mathrm{K}_1(F[x]) \simeq F^{\cdot} \simeq \mathrm{K}_1(F),\quad 其中F为域,$$

因此 $\mathrm{K}_1(\mathbb{F}_{p^n}[x])\simeq \mathbb{Z}_{p^n-1}$，其中 $\mathbb{F}_{p^n}$ 表示 p^n 个元素有限域。

由命题6.1之证中的(＊)式又可得：

命题6.2 设 $R\in \mathfrak{R}\mathrm{ing}$，则

(1) $R\in \mathrm{GE}_n \Leftrightarrow \forall A\in \mathrm{GL}_n(R)$，$A=BD$，其中 $B\in \mathrm{E}_n(R)$，$D=\mathrm{diag}(d,1,\cdots,1)$，$d\in R^{\cdot} \Leftrightarrow \forall A\in \mathrm{GL}_n(R)$，$A=D_1 B_1$，其中 $B_1\in \mathrm{E}_n(R)$，$D_1=\mathrm{diag}(d_1,1,\cdots,1)$，$d_1\in R^{\cdot}$；

(2) $R\in \mathrm{GE} \Leftrightarrow \forall n, A\in \mathrm{GL}_n(R)$，$A=BD$，其中 $B\in E_n(R)$，$D=\mathrm{diag}(d,1,\cdots,1)$，$d\in R^{\cdot} \Leftrightarrow \forall n, A\in \mathrm{GL}_n(R)$，$A=D_1 B_1$，其中 $B_1\in \mathrm{E}_n(R)$，$D_1=\mathrm{diag}(d_1,1,\cdots,1)$，$d_1\in R^{\cdot}$。

证 显然只需证(1)的第一个"⇔"中的"⇒"。事实上,由命题 6.1(3)知 $R\in GE_n\Leftrightarrow\forall A\in GL_n(R), A=B_2D_2$,其中 $B_2\in E_n(R), D_2=\mathrm{diag}(d_1,d_2,\cdots,d_n), d_j\in R^{\cdot}, j=1,2,\cdots,n$。取 $t_n=\mathrm{diag}(1,1,\cdots,1,d_n,d_n^{-1}), t_{n-1}=\mathrm{diag}(1,1,\cdots,d_nd_{n-1},(d_nd_{n-1})^{-1},1),\cdots,t_2=\mathrm{diag}(d_nd_{n-1}\cdots d_2,(d_nd_{n-1}\cdots d_2)^{-1},1,\cdots,1)$,由推论 5.1 即知 $t_j\in E_n(R), j=2,\cdots,n$。且

$$t_2t_3\cdots t_{n-1}t_nD_2=\mathrm{diag}(d,1,\cdots,1),$$

其中 $d=d_nd_{n-1}\cdots d_2d_1\in R^{\cdot}$。于是

$$D_2=t_n^{-1}t_{n-1}^{-1}\cdots t_2^{-1}\mathrm{diag}(d,1,\cdots,1), t_j^{-1}\in E_n(R)$$

代入 $A=B_2D_2$ 即得欲证。 □

推论 6.2 设 R 为除环,Euclid 环或局部环(未必交换),则 $\forall n, A\in GL_n(R)$ 时,必有 $A=BD$,其中 $B\in E_n(R), D=\mathrm{diag}(d,1,\cdots,1), d\in R^{\cdot}$。

由命题 6.2(2)知,若 $R\in GE$,则 $\forall n\geqslant 1, GL_n(R)=E_n(R)D_n(R)=D_n(R)E_n(R)$,令 $n\to\infty$ 则知

$$GL(R)=E(R)D(R)=D(R)E(R),$$

显然对 $R\in SGE$,此式也成立。其中 $D(R)=\mathrm{diag}(R^{\cdot},I_\infty)\simeq R^{\cdot}$(注意在此同构下,由推论 5.1(2),可认为 $[R^{\cdot},R^{\cdot}]\subset E(R)\cap D(R)$。

由于 $E(R)\lhd GL(R), D(R)<GL(R)$,由群的第二同构定理得

$$\begin{aligned}D(R)/(E(R)\cap D(R))&\simeq E(R)D(R)/E(R)\\&=GL(R)/E(R)=K_1(R)\end{aligned}$$

由此可得(注意 $R\in$ CRing 时,由引理 5.1 与定理 6.1(3)知 $E(R)\cap D(R)=\{I\}$,因此 $D(R)/E(R)\cap D(R)\simeq R^{\cdot}$):

定理 6.2 设 $R\in SGE$(R 未必为交换环),则

(1) $GL(R)=E(R)D(R)=D(R)E(R)$;

(2) $K_1(R)\simeq D(R)/(E(R)\cap D(R))\simeq R^{\cdot}/G$,其中 $[R^{\cdot},R^{\cdot}]<G<R^{\cdot}$;

(3) 有群的满同态

$$R^{\cdot ab}\equiv R^{\cdot}/[R^{\cdot},R^{\cdot}]\twoheadrightarrow K_1(R);$$

(4) 当 R 又为交换环时,$K_1(R)\simeq R^{\cdot}$。

由此知,若 R 为除环、Euclid 环或局部环(未必为交换环),则有群的满同态 $R^{\cdot ab}\twoheadrightarrow K_1(R)$,我们在后面的§8 中将对除环与局部环证明:事实上,有 $K_1(R)\simeq R^{\cdot ab}$。

再来讨论半局部环(如 Artin 环、半完全环、完全环、QF 环等)的 K_1 群,先证明一条引理。

引理 6.2 设 $R\in\mathbb{R}\text{ing}$，$K\lhd R$ 且 $K\subseteq J(R)$，则

(1) $R/K\in \mathrm{GE}_n \Leftrightarrow R\in \mathrm{GE}_n$；

(2) $R/K\in \mathrm{GE} \Leftrightarrow R\in \mathrm{GE}$；

(3) $R/K\in \mathrm{SGE} \Leftrightarrow R\in \mathrm{SGE}$。

证 只需证(1)，因为(1) $\Rightarrow$(2)，(3)都是显然的。

$\Rightarrow$：事实上，标准环同态 $\pi:R\to R/K$ 诱导出群同态

$$\mathrm{GL}_n(\pi):\mathrm{GL}_n(R)\to \mathrm{GL}_n(R/K)$$

（$K\not\subset J(R)$时未必为满同态，比如 $p>3$ 为素数，$\pi:\mathbb{Z}\twoheadrightarrow\mathbb{Z}/p\mathbb{Z}$ 诱导的 $\mathrm{GL}_1(\pi):\mathrm{GL}_1(\mathbb{Z})\to\mathrm{GL}_1(\mathbb{Z}/p\mathbb{Z})$即不是满同态）。显然

$$\mathrm{Ker}\mathrm{GL}_n(\pi)=I_n+K^{n\times n},$$

由 $K\subseteq J(R)$知 $1+a\in R^{\cdot}$，$\forall a\in K$，于是 $\mathrm{Ker}\mathrm{GL}_n(\pi)$中任一矩阵 $A=I_n+(a_{ij})$都是初等矩阵之积（用初等行变换(2)+(1)，(1)$-a_{11}(1+a_{11}+a_{21})^{-1}$(2)得(1,1)位置为 1 的新矩阵，再用初等行变换与归纳法即知）。因此

$$\mathrm{Ker}\mathrm{GL}_n(\pi)\subseteq \mathrm{GE}_n(R) \qquad (**)$$

任取 $C\in \mathrm{GL}_n(R)$，记 $\bar{C}=\mathrm{GL}_n(\pi)(C)$。由设用命题 6.2(1)可知，$\bar{C}=\bar{B}\,\bar{D}$，其中 $\bar{B}\in \mathrm{E}_n(R/K)$，$\bar{D}=\mathrm{diag}(\bar{d},1,\cdots,1)$，$\bar{d}\in(R/K)^{\cdot}$。由 $\mathrm{E}_n(\pi)(e_{ij}^r)=e_{ij}^{\bar{r}}$，$\bar{r}=\pi(r)$，知 $\mathrm{E}_n(\pi):\mathrm{E}_n(R)\to\mathrm{E}_n(R/K)$为满同态，因此必有 $B\in\mathrm{E}_n(R)$使 $\mathrm{E}_n(\pi)(B)=\bar{B}$。再取 $D=\mathrm{diag}(d,1,\cdots,1)$，其中 $\pi(d)=\bar{d}$。由 $\mathrm{Ker}\mathrm{GL}_n(\pi)=I_n+K^{n\times n}$知 C 与 BD 只相差一个因子 $E=I_n+F\in\mathrm{Ker}\mathrm{GL}_n(\pi)$，其中 $F\in K^{n\times n}$。于是由($**$)知有 $E\in\mathrm{GE}_n(R)$使 $C=BDE$ 或 EBD。由此知 $R\in \mathrm{GE}_n$。

$\Leftarrow$：只需证 $\mathrm{GL}_n(\pi)$是满的。事实上，任取 $\bar{A}\in\mathrm{GL}_n(R/K)$，则有 $\bar{B}\in\mathrm{GL}_n(R/K)$使 $\bar{A}\bar{B}=\bar{I}_n$。注意必有 $A,B\in \mathrm{M}_n(R)\equiv R^{n\times n}$使 $\mathrm{M}_n(\pi)(A)=\bar{A}$，$\mathrm{M}_n(\pi)(B)=\bar{B}$ 且 AB 的对角元都在 $1+K\subseteq R^{\cdot}$ 中，非对角元都在 K 中，于是对 AB 作初等列变换可化为 I_n，即有 $E\in\mathrm{E}_n(R)$使 $ABE=I_n$，因此 $A\in\mathrm{GL}_n(R)$，即 $\mathrm{GL}_n(\pi)$是满的。 □

由上证明顺便得：

推论 6.3 设 $R\in\mathbb{R}\text{ing}$，$K\lhd R$，$\pi:R\twoheadrightarrow R/K$ 为标准环同态，则 $\mathrm{E}_n(\pi)$是满同态，且当 $K\subseteq J(R)$时 $\mathrm{GL}_n(\pi)$也是满同态。

现在可证如下结果：

定理 6.3 设 R 为半局部环（未必为交换环），则

(1) $R\in\mathrm{GE}$；

(2) $\mathrm{K}_1(R)\simeq R^{\cdot}/G$，其中$[R^{\cdot},R^{\cdot}]<G<R^{\cdot}$；

(3) 有群的满态 $R^{\cdot ab} \twoheadrightarrow K_1(R)$;

(4) 当 R 是交换半局部环时,$K_1(R) \simeq R^{\cdot}$。

证 由 R 为半局部环知 $R/J(R)$ 为 Artin 半单环,于是由命题 6.1 知 $R/J(R) \in \mathrm{GE}$,因此由引理 6.2 知 $R \in \mathrm{GE}$,再由定理 6.2 即得(2),(3),(4)。 □

注③ 在§9 中我们将讨论对定理 6.2(2)中的 $K_1(R) \simeq R^{\cdot}/G$,并在 R 为半局部环时完全确定这个 G。

从定理 6.1 可知 求 K_1 群时判定出 $R \in \mathrm{SGE}$ 即已足够,不必再判定 $R \in \mathrm{GE}$,且判定 $R \in \mathrm{GE}$ 比判定 $R \in \mathrm{SGE}$ 困难得多。比如(见[McDonald, 1984]),对有限循环群 G,H. Bass 于 1967 年即证出$\mathbb{Z}G \in \mathrm{GE}_n$, $\forall n \geqslant 3$。从而$\mathbb{Z}G \in \mathrm{SGE}$,但直到 1984 年,K. Dennis,B. Magurn 与 L. Vaserstein 才证出$\mathbb{Z}G \in \mathrm{GE}_2$,此时才知$\mathbb{Z}G \in \mathrm{GE}$。当然,判定 $R \in \mathrm{SGE}$ 也不是容易的,不过,交换 GE 环有一个子类——交换稳定环是比较容易判定的。

定义 6.2 设 $R \in \mathfrak{Ring}$,且 $aR+bR=R$(即有 $x,y \in R$ 使 $ax+by=1$,此时称(a,b)为二元幺模行(列),记为$(a,b) \in U_2(R)$)时必有 $c \in R$ 使 $a+bc$ 有右逆元(在 R 中),则称 R 为**稳定环**(stable ring)或**稳定度为 1 的环**,记为 $R \in \mathrm{Sr}1$。

这是 H. Bass 在[Bass, 1964]中给出的定义,也是 1967 年 D. Estes 与 J. Ohm 对交换环所作定义的依据。更一般地,在 $\mathfrak{M}_R$ 中若对 $X=(x_1,\cdots,x_m) \in R^{1\times m}$,$x_1R+\cdots+x_mR=R$,则称 X 为 m 元**幺模行**,记为 $X \in U_m(R)$(为方便起见,也记为 $X^T \in U_m(R)$)。如果对 $X=(x_1,\cdots,x_{m+1}) \in U_{m+1}(R)$ 有 $y_1,\cdots,y_m \in R$ 使$(x_1+x_{m+1}y_1, x_2+x_{m+1}y_2,\cdots,x_m+x_{m+1}y_m) \in U_m(R)$,则称 X **可缩短**(reduced)或称 X 为**稳定的**(stable)。记

$$\mathrm{Sr}(R) = n \equiv \min\{m \mid \forall Y \in U_{m+1}(R) \text{ 都可缩短}\},$$

称为 R 的**(右)稳定度**(stable range)。可类似地定义左稳定度且可证 R 的左、右稳定度是相等的(见[McConnell, 1988]),都可记为 $\mathrm{Sr}(R)=n$ 或 $R \in \mathrm{Sr}n$。

现证明定义 6.2 中"$a+bc$ 有右逆元"等价于"$a+bc \in R^{\cdot}$"。为此只需证:

命题 6.3 设 $R \in \mathrm{Sr}1$,则 R 为 Dedekind 有限环(直有限环),即 R 中 $uv=1$ 与 $vu=1$ 是等价的。

证 只需证 $uv=1$ 时 $u \in R^{\cdot}$。事实上,由$(v,1-vu) \in U_2(R)$知,必有 $t \in R$ 使 $x \equiv v+(1-vu)t$ 有右逆元 x_r^{-1}。而 $ux=uv+ut-uvut=uv=1$,于是 u 又是 x 的左逆元,因此 $x \in R^{\cdot}$。由此知 $u \in R^{\cdot}$。 □

1973 年 E. G. Evans 证明了：$\mathrm{End}_R(M)\in \mathrm{Sr1}$ 时 M 在$_R\mathfrak{M}$ 中直和可消，即 $M\oplus B\simeq M\oplus C$ 时必有 $B\simeq C$（在$_R\mathfrak{M}$ 中）（见[Menal,1988]）。于是 $R\in$ Sr1 时，R 在$_R\mathfrak{M}$ 中直和可消（反之不真，如由$(2,5)\in \mathrm{U}_2(\mathbb{Z})$不可缩短知，$\mathbb{Z}\notin$ Sr1，但$\mathbb{Z}$在$_{\mathbb{Z}}\mathfrak{M}$ 中直和可消）。因此 Sr1 环类的判定是直和消去理论中的重要课题，它与 K_0、K_1 群都有密切的关系。可以证明 Sr1 环类对环的直积及正向极限$\varinjlim$都是封闭的，且 $R/J(R)\in \mathrm{Sr1}\Leftrightarrow R\in \mathrm{Sr1}\Leftrightarrow R^{n\times n}\in \mathrm{Sr1}$，$\forall n\geq 1$，因此半局部环必是稳定度为 1 的环。幺正则环（满足条件：$\forall r\in R$，必有 $u\in R^{\cdot}$ 使 $rur=r$ 的环 R 称为幺正则环）即稳定度为 1 的 von Neumann 正则环，Krull 维数为 0 的环以及稳定度为 1 的环上的形式幂级数环等都是稳定度为 1 的环，但对任意交换环 R，$R[x]\notin \mathrm{Sr1}$（(x,x^2+1)不可缩短）。现在我们对 IBN 环来考察 Sr1，SFF，GE 的关系，为此先建立一条有用的引理。

引理 6.3 设 $R\in$ IBN，则下三点等价：

(1) $R\in$ SFF；

(2) 设 $f:R^n\twoheadrightarrow R$ 为 $\mathfrak{M}_R$ 中任一满同态，$\pi:R\oplus R^{n-1}\twoheadrightarrow R$ 为 $\mathfrak{M}_R$ 中对第一直和项的标准投射（同态），则有 $\mathfrak{M}_R$ 中的同构 $\bar{f}:R^n\to R\oplus R^{n-1}$使 $\pi\bar{f}=f$；

(3) $R\in$ UCP（即 R 为有幺模列（行）性质的环，意指：$\forall (a_1,\cdots,a_n)^T\in \mathrm{U}_n(R)$（$(a_1,\cdots,a_n)\in \mathrm{U}_n(R)$）都有 $A\in \mathrm{GL}_n(R)$ 以 $(a_1,\cdots,a_n)^T$（$(a_1,\cdots,a_n)$）为其第 1 列（行））。

证 (1) $\Rightarrow$(2)：设 $R\in$ SFF，令 $P=\mathrm{Ker}f$ 则由 $R\in \mathrm{P}\mathfrak{M}_R$ 知，在同构意义下可认为 $R^n=R\oplus P$，于是 f 可看成是 $R\oplus P$ 关于第一直和项的投射：即 $f|_R=I_R$。由 $R\in$ IBN 且 $R\in$ SFF 知有 $\mathfrak{M}_R$ 同构 $g:P\to R^{n-1}$，因此 $f|_R\oplus g$：$R\oplus P=R^n\to R\oplus R^{n-1}$为同构，记 $\bar{f}=f|_R\oplus g$，显然有 $\pi\bar{f}=f$。

(2) $\Leftrightarrow$(3)：设(2)成立，任取$(x_1,\cdots,x_n)\in \mathrm{U}_n(R)$，则 $A=(x_1,x_2,\cdots,x_n)^T\in R^{n\times 1}$对应的 $f:R^n\to R$ 为满同态（R^n 中元素视为行向量，$f(Y)=YA$，$\forall Y\in R^n$）。π 对应的矩阵显然为$(1,0,\cdots,0)^T\in R^{n\times 1}$，记 $\bar{A}\in R^{n\times n}$为 $\bar{f}$ 对应的矩阵。(2)成立时，由 $\bar{f}$ 为同构知 $\bar{A}\in \mathrm{GL}_n(R)$，而由 $\pi\bar{f}=f$ 又知 $\bar{A}(1,0,\cdots,0)^T=A$，即$(x_1,\cdots,x_n)^T$ 为 $\bar{A}\in \mathrm{GL}_n(R)$的第 1 列，因此 $R\in$ UCP，即(2) $\Rightarrow$(3)。

反过来若(3)成立，满同态 $f:R^n\to R$ 对应的 A 必为幺模列，由 $R\in$ UCP 知 A 必为某一个 $\bar{A}\in \mathrm{GL}_n(R)$的第 1 列，令 $\bar{A}$ 对应的同态为 $\bar{f}:R^n\to R\oplus R^{n-1}$，则 $\bar{f}$ 为同构且 $\bar{A}(1,0,\cdots,0)^T=A$，即 $\pi\bar{f}=f$。因此(2)成立。

(2)$\Rightarrow$(1)：设 $R\oplus P\simeq R^n$，令 $f:R^n=R\oplus P\to R$ 为对应第一直和项的标

准投射。由(2)知必有同构 $\bar{f}: R^n \to R \oplus R^{n-1}$ 使 $\pi\bar{f} = f$，由 $\bar{f}$ 为同构知 $P \equiv \mathrm{Ker}f \simeq \mathrm{Ker}\pi = R^{n-1}$。用归纳法即知，更一般地，$R^r \oplus Q \simeq R^n$ 蕴含着 $Q \simeq R^{n-r}$（注意 $R \in \mathrm{IBN}$），故 $R \in \mathrm{SFF}$。 □

命题 6.4　设 $R \in \mathrm{Sr1}$，则

(1) $R \in \mathrm{SFF} = \mathrm{UCP}$；

(2) $R \in \mathrm{GE}$，因此有群的满同态 $R^{\cdot ab} \twoheadrightarrow K_1(R)$，且当 $R \in \mathrm{CRing}$ 时 $K_1(R) \simeq R^{\cdot}$。

证　(1) 由 $R \in \mathrm{Sr1}$，可证 $R \in \mathrm{IBN}$，再由引理 6.3 知，只需证 $R \in \mathrm{UCP}$。任取 $n \geqslant 2$ 与 $(a_1, a_2, \cdots, a_n) \in U_n(R)$，即有 $b_1, \cdots, b_n \in R$ 使 $a_1b_1 + \cdots + a_nb_n = 1$。可视为 $(a_1, a_2b_2 + \cdots + a_nb_n) \in U_2(R)$，由 $R \in \mathrm{Sr1}$ 知必有 $c \in R$ 使

$$a_1 + (a_2b_2 + \cdots + a_nb_n)c = u \in R^{\cdot}\ (\text{由命题 6.3})。$$

记 $c_j = b_jc$，则 $a_1 + a_2c_2 + \cdots + a_nc_n = u$，对

$$A = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ -c_2 & 1 & & \\ \cdots & & \ddots & \\ -c_n & & & 1 \end{pmatrix}$$

作初等行变换 $(1) - \sum_{i=2}^{n} a_i(i)$，再作初等行变换 $(i) + c_iu^{-1}(1), i = 2, \cdots, n$，则 A 变为 $\mathrm{diag}(u, 1, \cdots, 1)$。于是 $A \in GL_n(R)$ 且以 $(a_1, a_2, \cdots, a_n)$ 为第 1 行，故 $R \in \mathrm{UCP}$。

(2) 任取 n 与

$$A = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ & & * & \end{pmatrix} \in GL_n(R)$$

记 A^{-1} 的第 1 列为 $(b_1, b_2, \cdots, b_n)^T$ 由 $AA^{-1} = I_n$ 知

$$a_1b_1 + a_2b_2 + \cdots + a_nb_n = 1。$$

由 $R \in \mathrm{Sr1}$，仿上段证明知必有 $c_2, \cdots, c_n \in R$ 使

$$a_1 + a_2c_2 + \cdots + a_nc_n = u \in R^{\cdot}。$$

记

$$C = \begin{pmatrix} 1 & & & \\ c_2 & 1 & & \\ \cdots & & \ddots & \\ c_n & & & 1 \end{pmatrix},$$

则由引理 5.4 知 $C \in E_n(R)$。而 AC 的 $(1,1)$ 元素为 $u \in R^{\cdot}$，因此 $AC \equiv (c_{ij})$

可经行列初等变换$(i)-c_{i1}u^{-1}(1)$，$\widehat{j}-c_{1j}u^{-1}\widehat{1}$，$i,j=2,\cdots,n$变成

$$\begin{pmatrix} u & \\ & A_1 \end{pmatrix} \in \mathrm{GL}_n(R),$$

其逆矩阵必为

$$\begin{bmatrix} u^{-1} & \\ & B_1 \end{bmatrix} \text{形且 } A_1B_1 = B_1A_1 = I_{n-1}$$

因此$A_1\in \mathrm{GL}_{n-1}(R)$。用归纳法即可将$A$用初等行、列变换化为可逆对角形，故$R\in \mathrm{GE}$。由定理 6.2 又可得关于$\mathrm{K}_1(R)$的相应结果。 □

由引理 6.3，命题 6.4 及命题 1.7 立得：

推论 6.4 设$R\in \mathrm{Sr}1$且$\mathrm{K}_0(R)\overset{f}{\simeq}\mathbb{Z}$，使$f([R])=1$，则$R\in \mathrm{PF}$。

命题 6.4 又可以被改进为：

定理 6.4 设$R\in \mathrm{IBN}$，则下面五点有关系：

$$(1)\Leftrightarrow(2)\Rightarrow\begin{cases}(3)\Leftrightarrow(4)\\(5)\end{cases}$$

(1) $\mathrm{Sr}(R)\leqslant n$，$1\leqslant n<\infty$；

(2) $\forall(a_1,a_2,\cdots,a_{m+1})\in \mathrm{U}_{m+1}(R)$都是可缩短的，因此$\mathrm{Sr}m\supseteq \mathrm{Sr}n$，$\forall m\geqslant n$；

(3) $\forall(a_1,a_2,\cdots,a_{m+1})\in \mathrm{U}_{m+1}(R)$都可作为一个$A\in \mathrm{GL}_{m+1}(R)$的第 1 行，$\forall m\geqslant n$；

(4) 在($\mathfrak{M}_R$中)$P\oplus R^s\simeq R^t$，$t-s=m$时，$P\simeq R^m$，$\forall m\geqslant n$，因此秩不小于n的稳定自由模都是有限生成自由模；

(5) $\mathrm{K}_1(R)$由$\mathrm{GL}_n(R)$在$\mathrm{GL}(R)$中的象$\mathrm{mod}\mathrm{E}(R)$生成，当$R\in \mathrm{CRing}$时$\mathrm{K}_1(R)$由$R^{\cdot}=\mathrm{GL}_1(R)$与$\mathrm{SL}_n(R)$在$\mathrm{GL}(R)$中的象$\mathrm{mod}\mathrm{E}(R)$生成。

证 (1)⇒(2)：由归纳法知只需证$m=n+1$的情况。任取$(a_1,a_2,\cdots,a_{n+2})\in \mathrm{U}_{n+2}(R)$，则有$b_j\in R$，$j=1,\cdots,n+2$使$\sum_{j=1}^{n+2}a_jb_j=1$，记$a'=a_{n+1}b_{n+1}+a_{n+2}b_{n+2}$，则显然有$(a_1,\cdots,a_n,a')\in \mathrm{U}_{n+1}(R)$，于是由$R\in \mathrm{Sr}n$知必有$r_1,\cdots,r_n\in R$使$(a_1+a'r_1,\cdots,a_n+a'r_n)\in U_n(R)$。由此不难看出

$$\begin{aligned}&(a_1+a_{n+2}b_{n+2}r_1,\cdots,a_n+a_{n+2}b_{n+2}r_n,\\&a_{n+1}+a_{n+2}\cdot 0)\in \mathrm{U}_{n+1}(R)\end{aligned}$$

即$(a_1,a_2,\cdots,a_{n+2})$是可缩短的。

(2)⇒(1)显见的。

(2)⇒(3)：只需证$m=n$的情况即可得证。

首先注意 $U_{n+1}(R)$ 中的分量作置换后仍属于 $U_{n+1}(R)$(一般地,可能影响其缩短性,如 $(5,2)\in U_2(\mathbb{Z})$ 可缩短,但 $(2,5)\in U_2(\mathbb{Z})$ 不可缩短。不过,由(2)知 $U_{n+1}(R)$ 中向量均可缩短,作此置换后不影响本证明的一般性)。于是任取 $(a_1,a_2,\cdots,a_{n+1})\in U_{n+1}(R)$,其缩短形可取为 $(a_2+a_1r_1,a_3+a_1r_2,\cdots,a_{n+1}+a_1r_n)\in U_n(R)$。与此相应地有初等列变换

$$(a_1,a_2,\cdots,a_{n+1})\xrightarrow[i=2,3,\cdots,n+1]{\hat{i}+\hat{1}\ r_{i-1}}(a_1,a_2+a_1r_1,\cdots,a_{n+1}+a_1r_n)$$

于是有初等阵 $T_1\in E_{n+1}(R)$ 使 $(a_1,a_2,\cdots,a_{n+1})T_1=(a_1,a_2+a_1r_1,\cdots,a_{n+1}+a_1r_n)$。由 $(a_2+a_1r_1,a_3+a_1r_2,\cdots,a_{n+1}+a_1r_n)\in U_n(R)$ 知,必有 $c_j\in R$ 使 $(a_2+a_1r_1)c_2+\cdots+(a_{n+1}+a_1r_n)c_{n+1}=1$,于是上式右边又可经 $\hat{1}+\sum_{i=2}^{n+1}\hat{i}\ c_i(1-a_i)$ 的初等列变换变为 $(1,a_2+a_1r_1,\cdots,a_{n+1}+a_1r_n)$。再用初等列变换 $\hat{i}-\hat{1}\ (a_i+a_1r_{i-1}),i=2,\cdots,n+1$,即化为 $(1,0,\cdots,0)$,于是有 $T_2\in E_{n+1}(R)\subset GL_{n+1}(R)$ 使

$$(a_1,a_2,\cdots,a_{n+1})T_2=(1,0,\cdots,0)$$

因此 $(a_1,a_2,\cdots,a_{n+1})=(1,0,\cdots,0)T_2^{-1}$ 为 $T_2^{-1}\in GL_{n+1}(R)$ 的第1行。

(3)⇒(4)由上段(2)⇒(3)之证可知(注意 $(e_{ij}^a)^T=e_{ji}^a$):$\forall m\geqslant n$,$(a_1,a_2,\cdots,a_{m+1})^T\in U_{m+1}(R)$ 都是某一个 $A\in GL_{m+1}(R)$ 的第1列。由引理6.3之证的方法知,$(a_1,a_2,\cdots,a_{m+1})^T$ 对应 $\mathfrak{M}_R$ 中一个满同态 $f:R^{m+1}\twoheadrightarrow R$。关于第一直和项的标准投射 $\pi:R\oplus R^m\twoheadrightarrow R$ 对应着 $(1,0,\cdots,0)^T$,而 A 则对应着同构:$\bar{f}:R^{m+1}\to R\oplus R^m$ 使 $\pi\bar{f}=f$,于是由引理6.3之证并用归纳法即知,秩不小于 n 的稳定自由模 P(作为 $\mathrm{Ker}f$)都是有限生成自由的。

(4)⇒(3):任取 $(a_1,\cdots,a_{m+1})\in U_{m+1}(R)$,必有 $b_1,\cdots,b_{m+1}$ 使 $\sum_{i=1}^{m+1}a_ib_i=1$(注意由 $\mathrm{Sr}n$ 的左右对称性,这里在 ${}_R\mathfrak{M}$ 中论证)。于是有对应于 $(a_1,\cdots,a_{m+1})^T$ 的满同态 $f:R^{m+1}\twoheadrightarrow R$,记 $P=\mathrm{Ker}f$,则 $P\oplus R\simeq R^{m+1}$,由(4)知 $P\simeq R^m$。定义 $\pi:R\oplus R^m\twoheadrightarrow R$ 为关于第一直和项的投射,即 π 对应 $(1,0,\cdots,0)^T$,则有同构 $\bar{f}:R^{m+1}\to R\oplus R^m$,$\bar{f}$ 对应 $\bar{A}\in GL_{m+1}(R)$ 且 $\pi\bar{f}=f$,于是 $(a_1,\cdots,a_{m+1})^T$ 为 $\bar{A}$ 的第1列,即 $(a_1,\cdots,a_{m+1})$ 为 $\bar{A}^T\in GL_{m+1}(R)$ 的第1行。

(2)⇒(5):任取 $A=(a_{ij})\in GL_{m+1}(R)$,则 $A_{\hat{1}}=(a_{11},a_{21},\cdots,a_{m+1,1})^T\in U_{m+1}(R)$,由(2)注意 $\mathrm{Sr}n$ 的左右对称性,知 $A_{\hat{1}}$ 是可缩短的。于是仿(2)⇒(3)之证知,有 $T_2\in E_{m+1}(R)$ 使

$$T_2A = \begin{pmatrix} 1 & * \\ & * \end{pmatrix}$$

对 T_2A 作初等列变换(对应 $T_3 \in E_{m+1}(R)$)则可使

$$T_2AT_3 = \begin{pmatrix} 1 & \\ & A_1 \end{pmatrix},$$

其逆矩阵必为

$$\begin{pmatrix} 1 & \\ & B_1 \end{pmatrix}$$

形,因此 $A_1 \in \mathrm{GL}_m(R)$。依此类推知必有 $T_4, T_5 \in \mathrm{E}_{m+1}(R)$使

$$T_4AT_5 = \begin{pmatrix} 1 & & & \\ & \ddots & & \\ & & 1 & \\ & & & A_2 \end{pmatrix},$$

其中 $A_2 \in \mathrm{GL}_n(R)$。于是 $\mathrm{K}_1(R)$由 $\mathrm{GL}_n(R)$在 $\mathrm{GL}(R)$中的象 $\mathrm{mod}\,\mathrm{E}(R)$生成。当 $R \in \mathcal{C}\mathrm{Ring}$ 时,由引理 5.1 知 $\mathrm{K}_1(R)$由 $R^{\cdot} = \mathrm{GL}_1(R)$与 $\mathrm{SL}_n(R)$在 $\mathrm{GL}(R)$中的象 mod $\mathrm{E}(R)$生成。 □

利用引理 6.3 前所述结果:半局部环为稳定度为 1 的环,立得

推论 6.5 设 R 为半局部环(未必交换),更一般地,$R \in \mathrm{Sr}1$,则 $\mathrm{K}_1(R)$由 $R^{\cdot} = \mathrm{GL}_1(R)$在 $\mathrm{GL}(R)$中的象 $\mathrm{mod}\,E(R)$生成。当 R 又是交换环时,又有 $\mathrm{K}_1(R) \simeq R^{\cdot}$。

§7 Dedekind 环的 K_1 群与 Mennicke 符号

如众周知,代数数域 F(有理数域$\mathbb{Q}$的有限扩张域)中的代数整元环 O_F 为 Dedekind 环,在代数数论中起着重要的作用。在代数几何中,平面代数曲线 l 无奇点(光滑)的充要条件是 l 的坐标环为 Dedekind 环(见[Orzech, 1981])。最常用的整数环$\mathbb{Z}$,以及更一般的 PID 都是 Dedekind 环,因此 Dedekind 环的重要地位是不容置疑的。Dedekind 环有两个常用的特征性质:① 一切非零真理想都可惟一地分解为极大理想幂的乘积;② 一切非零理想都可逆(详见§22)。为研究 Dedekind 环的 K_1 群,先证明如下结果:

命题 7.1 设 R 为 Dedekind 环,则 $\mathrm{Sr}(R) \leqslant 2$,即,Dedekind 环的稳定度不超过 2。

证 只需证任意的幺模行 $\alpha = (a_1, a_2, a_3) \in \mathrm{U}_3(R)$都可缩短,令 $I =$

$a_3R \lhd R$。

(1) 当 $I=0$,即 $a_3=0$ 时 $(a_1+a_3\cdot 0, a_2+a_3\cdot 0)=(a_1,a_2)\in U_2(R)$,无需再证。

(2) 当 $I=R$,即 a_3 有逆元 $a_3^{-1}\in R$ 时,$(a_1+a_3(1-a_3^{-1}a_1), a_2+a_3\cdot 0)=(a_3,a_2)\in U_2(R)$,即 α 可缩短。

(3) 当 $0\neq I\neq R$ 时,由 Dedekind 环的性质知,必有 $M_j\in \mathrm{Max}R$ 使

$$I = M_1^{n_1}\cdots M_k^{n_k},\ M_1,\cdots,M_k\ \text{互异。}$$

于是 R/I 为交换局部环的直积(由中国剩余定理):

$$R/I \simeq R/M_1^{n_1}\oplus\cdots\oplus R/M_k^{n_k}\text{。}$$

由推论 6.1 知 $SL_n(R/M_j^{n_j})=E_n(R/M_j^{n_j})$,$j=1,2,\cdots,k$。因此

$$SL_n(R/I) = E_n(R/I),\qquad \forall n\geqslant 2$$

记 $x\in R$ 在标准环同态 $\pi: R\twoheadrightarrow R/I$ 下的象为 $\bar{x}$。由 $\alpha\in U_3(R)$ 知,$a_1R+a_2R+a_3R=R$。因此

$$\begin{aligned}&\bar{a}_1R/I+\bar{a}_2R/I+\bar{a}_3R/I\\&=\bar{a}_1R/I+\bar{a}_2R/I\\&=R/I(\text{注意 } a_3\in I,\bar{a}_3=\bar{0})\end{aligned}$$

于是有 $\bar{x}_1,\bar{x}_2\in R/I$ 使 $\bar{a}_1\bar{x}_1+\bar{a}_2\bar{x}_2=\bar{1}$(即 $a_1x_1+a_2x_2-1\in I$),因此

$$\det\begin{pmatrix}\bar{x}_1 & \bar{x}_2\\ -\bar{a}_2 & \bar{a}_1\end{pmatrix}=\bar{1}$$

由此知

$$\begin{pmatrix}\bar{x}_1 & \bar{x}_2\\ -\bar{a}_2 & \bar{a}_1\end{pmatrix}\in SL_2(R/I) = E_2(R/I)$$

注意 π 诱导的群同态 $E_n(\pi): E_n(R)\twoheadrightarrow E_n(R/I)$)(使 $e_{ij}^a\mapsto e_{ij}^{\bar{a}}$)必为满同态($GL_n(\pi): GL_n(R)\to GL_n(R/I)$,$SL_n(\pi): SL_n(R)\to SL_n(R/I)$ 未必为满同态)。因此 $E_2(R/I)$ 的上述矩阵在 $E_2(R)$ 中有关于 $E_2(\pi)$ 的原象,且让 $\bar{a}_2$,$\bar{a}_1$ 各取适当的代表元 b_2,b_1,可取此原象为

$$\begin{pmatrix}x_1 & x_2\\ -b_2 & b_1\end{pmatrix}\in E_2(R)\subset SL_2(R)$$

于是 $b_1x_1+b_2x_2=1$。又 $a_1x_1+a_2x_2-1\in I=a_3R$,因此有 $x_3\in R$ 使 $a_1x+a_2x_2+a_3x_3=1$。注意到

$$x_3 = 1\cdot x_3 = (b_1x_1+b_2x_2)x_3,$$

则有

$$a_1x_1+a_2x_2+a_3(b_1x_1+b_2x_2)x_3 = 1,$$

即

$$(a_1+a_3b_1x_3)x_1+(a_2+a_3b_2x_3)x_2=1$$

于是

$$(a_1+a_3b_1x_3,a_2+a_3b_2x_3)\in U_2(R),$$

即 α 可缩短。因此 $Sr(R)\leqslant 2$。 □

由下述推论知命题 7.1 不能再改进为 $Sr(R)=1$。但由上证知，命题 7.1可推广到“一切主理想都是极大理想幂之乘积”的交换环。

推论 7.1 $Sr(\mathbb{Z})=2$。

证 由 $\mathbb{Z}$ 为 Dedekind 环由命题 7.1 知 $Sr(\mathbb{Z})\leqslant 2$，但 $(2,5)\in U_2(\mathbb{Z})$ 不可缩短，因此 $Sr(\mathbb{Z})=2$。

由命题 7.1 与定理 6.4 再注意到引理 5.1，即得 Dedekind 环 K_1 群的下述结果。

定理 7.1 设 R 为 Dedekind 环，则 $K_1(R)$ 由 $GL_1(R)=R^{\cdot}$ 与 $SL_2(R)$ 在 $GL(R)$ 中的象 mod $E(R)$ 生成，因此也可由 $GL_2(R)$ 在 $GL(R)$ 中的象 mod $E(R)$ 生成，即

$$\begin{aligned}K_1(R)&=\left\langle\begin{pmatrix}R^{\cdot}&\\&I_\infty\end{pmatrix}\bmod E(R),\begin{pmatrix}SL_2(R)&\\&I_\infty\end{pmatrix}\bmod E(R)\right\rangle\\&=\begin{pmatrix}GL_2(R)&\\&I_\infty\end{pmatrix}\bmod E(R)\\&\simeq R^{\cdot}\oplus\begin{pmatrix}SL_2(R)&\\&I_\infty\end{pmatrix}\bmod E(R)\end{aligned}$$

注① 由于 1974 年 H. Bass 已给出一个 $R\in$ PID 使 $SL_2(R)\neq E_2(R)$，因此定理 7.1 已不能再作实质上的改进。此外注意到 $\mathbb{Z}^{\cdot}=\{\pm 1\}$，由定理 7.1 又一次看出 $K_1(\mathbb{Z})\simeq\mathbb{Z}_2$（2 阶循环群）。

由定理 7.1 还可以看出，对交换环 R 研究 $SL_2(R)$ 在 $GL(R)$ 中的象 mod $E(R)$ 生成的 $SK_1(R)$ 的子群（当然也是 $K_1(R)$ 的子群）；找出该子群中元素便于计算的表示形式，都是十分有意义的，尤其是对 Dedekind 环。为此我们通过下述引理介绍 Mennicke 符号（Mennicke symbol）。

首先注意

$$\begin{pmatrix}a&b\\c&d\end{pmatrix}\in SL_2(R)$$

意味着 $(a,b)\in U_2(R)$ 且作 $(2)+r(1)$，$\forall r\in R$ 所得的新矩阵第 1 行仍为 (a,b)，第 2 行则变成 $(c+ra,d+rb)$，新矩阵 mod $E(R)$（即对应 $SK_1(R)$ 中的元素）与原矩阵 mod $E(R)$ 仍相同。即

$$\overline{\begin{pmatrix} a & b \\ c & d \end{pmatrix}} = \overline{\begin{pmatrix} a & b \\ c+ra & d+rb \end{pmatrix}} \pmod{E(R)}$$

于是容易联想到去试证下述引理。

引理 7.1　设 $R\in\mathcal{C}\text{Ring}$，$(a,b)\in U_2(R)$，则 $SL_2(R)$ 中以 (a,b) 为第 1 行的矩阵一定存在，且这些矩阵(在 $GL(R)$ 中的象) mod $E(R)$ 的同余类($SK_1(R)$ 中的元素)与它们的第 2 行选取无关，记该同余类为 $[a\ b]$，称为 **Mennicke 符号**。

证　由 $(a,b)\in U_2(R)$ 知必有 $c,d\in R$ 使 $ad-bc=1$，因此

$$A=\begin{pmatrix} a & b \\ c & d \end{pmatrix}\in SL_2(R)$$

若又有

$$A_1=\begin{pmatrix} a & b \\ c' & d' \end{pmatrix}\in SL_2(R),$$

则 $\det A_1=ad'-bc'=1$。因此

$$A_1^{-1}=\begin{pmatrix} d' & -b \\ -c' & a \end{pmatrix},$$

且

$$AA_1^{-1}=\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} d' & -b \\ -c' & a \end{pmatrix}=\begin{pmatrix} 1 & \\ ad'-c'd & 1 \end{pmatrix}\in E_2(R)$$

所以 A,A_1(在 $GL(R)$ 中的象) mod $E(R)$ 的同余类相同。　□

由此可将定理 7.1 写为

定理 7.1′　设 R 为 Dedekind 环，则

$$SK_1(R)=\langle\{[a\ b]\mid(a,b)\in U_2(R)\}\rangle$$

因此

$$K_1(R)\simeq R^{\cdot}\oplus\langle\{[a\ b]\mid(a,b)\in U_2(R)\}\rangle$$

现在，我们给出下述结果以方便 Mennicke 符号的计算。

定理 7.2　设 $R\in\mathcal{C}\text{Ring}$，$(a,b)\in U_2(R)$，则 $[a\ b]\in SK_1(R)\subset K_1(R)$ 具有如下性质：

(1) 若 a 或 $b\in R^{\cdot}$，则 $[a\ b]=1$($SK_1(R)$ 的单位元)，即

$$[R^{\cdot}\ R]=[R\quad R^{\cdot}]=1;$$

(2) $[a\ b]=[b\ a]=[-b\ a]=[b\ -a]=[-a\ -b]$(对称性与反对称性)，

$$[a\ b]=[a+rb\ b]=[a\ b+ra],\ \forall r\in R;$$

(3) 若 $(a_1a_2,b)\in U_2(R)$，则 $(a_1,b),(a_2,b)\in U_2(R)$ 且 Mennicke 符号

有双乘性：

$$[a_1\ b][a_2\ b]=[a_1a_2\ b],$$
$$[b\ a_1][b\ a_2]=[b\ a_1a_2],$$

因此

$$[au\ b]=[a\ b]=[a\ bu],\ \forall u\in R^{\cdot},$$
$$[a\ b]^n=[a^n\ b]=[a\ b^n]。$$

特别地，

$$[a\ b]=[\pm a\ \pm b]=[\pm b\ \pm a]$$

证 (1) 令

$$A=\begin{pmatrix}a & b\\ c & d\end{pmatrix}\in \mathrm{SL}_2(R)$$

则 $a\in R^{\cdot}$ 时(用推论 5.1)，

$$A\xrightarrow[(2)-ca^{-1}(1)]{}\begin{bmatrix}a & b\\ & d-bca^{-1}\end{bmatrix}=\begin{bmatrix}a & b\\ & (ad-bc)a^{-1}\end{bmatrix}$$
$$=\begin{bmatrix}a & b\\ & a^{-1}\end{bmatrix}\xrightarrow[\text{左乘}\begin{pmatrix}a^{-1} & \\ & a\end{pmatrix}\in \mathrm{E}_2(R)]{}\begin{bmatrix}1 & a^{-1}b\\ & 1\end{bmatrix}\in \mathrm{E}_2(R)$$

因此 $A\in \mathrm{E}_2(R)$，即$[a\ b]=1$。

当 $b\in R^{\cdot}$ 时，

$$A\xrightarrow[(2)-db^{-1}(1)]{}\begin{bmatrix}a & b\\ c-adb^{-1} & \end{bmatrix}$$
$$=\begin{bmatrix}a & b\\ -b^{-1} & \end{bmatrix}\xrightarrow[(1)+ab(2)]{}\begin{bmatrix} & b\\ -b^{-1} & \end{bmatrix}\underset{(\text{推论}5.1)}{\in}\mathrm{E}_2(R)$$
$$\left(\begin{bmatrix}b^{-1} & \\ & b\end{bmatrix}\text{经三次行变换得}\begin{bmatrix} & b\\ -b^{-1} & \end{bmatrix}\right),$$

因此 $A\in \mathrm{E}_2(R)$，即$[a\ b]=1$。

(2) 由推论 5.1 知，作为 I_2 经三次行变换所得的

$$\begin{pmatrix} & 1\\ -1 & \end{pmatrix},\begin{pmatrix} & -1\\ 1 & \end{pmatrix}\in \mathrm{E}_2(R)$$

于是

$$\begin{pmatrix}a & b\\ c & d\end{pmatrix}\begin{pmatrix} & 1\\ -1 & \end{pmatrix}=\begin{pmatrix}-b & a\\ -d & c\end{pmatrix}\Rightarrow[a\ b]=[-b\ a]$$
$$\underset{\text{同理}}{=\!=}[-a\ -b]=[b\ -a]$$

$$\left(\text{或}\begin{pmatrix}a & b\\ c & d\end{pmatrix}\begin{pmatrix} & -1\\ 1 & \end{pmatrix}=\begin{pmatrix}b & -a\\ d & -c\end{pmatrix}\Rightarrow[a\ b]=[b\ -a]\right.$$

$$\left.\overset{\text{同理}}{=\!=\!=}[-a\ -b]=[-b\ a]\right);$$

$$\begin{pmatrix}a & b\\ c & d\end{pmatrix}\xrightarrow[\hat{1}\ +r\ \hat{2}]{}\begin{pmatrix}a+rb & b\\ c+rd & d\end{pmatrix}\Rightarrow[a\ b]=[a+rb\ b];$$

$$\begin{pmatrix}a & b\\ c & d\end{pmatrix}\xrightarrow[\hat{2}\ +r\ \hat{1}]{}\begin{pmatrix}a & b+ra\\ c & d+rc\end{pmatrix}\Rightarrow[a\ b]=[a\ b+ra]。$$

而$[a\ b]=[b\ a]$是(3)的特例(下段证(3)未用到$[a\ b]=[b\ a]$)。

(3) $(a_1a_2,\ b)\in U_2(R)$时,$(a_1,\ b)$,$(a_2,\ b)\in U_2(R)$是显见的。由(2)中已证的$[a\ b]=[b\ -a]$知,只需证$[a_1\ b][a_2\ b]=[a_1a_2\ b]$。

由于这里只需考虑各二阶矩阵在 $GL(R)$中的象 mod $E(R)$,因此,可让$[a_1\ b]$,$[a_2\ b]$分别对应 $SL_3(R)$中的

$$A_1=\begin{bmatrix}a_1 & b & 0\\ c_1 & d_1 & 0\\ 0 & 0 & 1\end{bmatrix},\ A_2=\begin{bmatrix}a_2 & b & 0\\ c_2 & d_2 & 0\\ 0 & 0 & 1\end{bmatrix}$$

且对 A_1,A_2 可任意左、右乘 $E_3(R)$中的矩阵(即对 A_1,A_2 作初等行、列变换)。但

$$A_2=\begin{bmatrix}a_2 & b & 0\\ c_2 & d_2 & 0\\ 0 & 0 & 1\end{bmatrix}\xrightarrow[\substack{\text{右乘}\begin{pmatrix}1&0&0\\0&0&1\\0&-1&0\end{pmatrix}\in E_3(R)\\ \hat{3}\ +\ \hat{2}\ .\ \hat{2}\ -\ \hat{3}\ ,\ \hat{3}\ +\ \hat{2}}]{}\begin{bmatrix}a_2 & 0 & b\\ c_2 & 0 & d_2\\ 0 & -1 & 0\end{bmatrix}$$

$$\xrightarrow[\substack{\text{左乘}\begin{pmatrix}1&0&0\\0&0&-1\\0&1&0\end{pmatrix}\\ ((3)+(2),(2)-(3),(3)+(2))}]{}\begin{bmatrix}a_2 & 0 & b\\ 0 & 1 & 0\\ c_2 & 0 & d_2\end{bmatrix}\equiv A_3,$$

即 $A_2\equiv A_3\bmod E(R)$。而

$$A_1A_3=\begin{bmatrix}a_1a_2 & b & a_1b\\ c_1a_2 & d_1 & c_1b\\ c_2 & 0 & d_2\end{bmatrix}\xrightarrow[\hat{3}\ -a_1\ \hat{2}]{}\begin{bmatrix}a_1a_2 & b & 0\\ c_1a_2 & d_1 & -1\\ c_2 & 0 & d_2\end{bmatrix}$$

$$\xrightarrow[\text{左乘}\begin{pmatrix}1&0&0\\0&0&1\\0&-1&0\end{pmatrix}\in E_3(R)]{}\begin{bmatrix}a_1a_2 & b & 0\\ c_2 & 0 & d_2\\ -c_1a_2 & -d_1 & 1\end{bmatrix}$$

$$\xrightarrow{\text{初等行、列变换}} \begin{pmatrix} a_1 a_2 & b & 0 \\ * & * & 0 \\ 0 & 0 & 1 \end{pmatrix} \equiv A_4 (\text{对应}[a_1 a_2\ b]),$$

因此，由 $A_2 \equiv A_3 \bmod \mathrm{E}(R)$ 知，

$$A_1 A_2 \equiv A_4 \bmod \mathrm{E}(R),$$

于是$[a_1\ b][a_2\ b]=[a_1 a_2\ b]$。 □

关于 $\mathrm{SK}_1(R)$的挠性，我们有下述结果：

命题 7.2 设 R 为 Dedekind 环，且 R/M 为有限域（即$|R/M|<\infty$），$\forall M \in \mathrm{Max}R$，则 $\mathrm{SK}_1(R)$为挠群。

证 $\forall (a,b) \in \mathrm{U}_2(R)$，考察$[a\ b]$。

(1) $b=0$ 时，必有 $a \in R^{\cdot}$，因此由定理 7.2(1)知$[a\ b]=1$。

(2) $b \in R^{\cdot}$ 时由定理 7.2(1)也知$[a\ b]=1$。

(3) $b \neq 0$ 且 $b \notin R^{\cdot}$ 时，$0 \neq Rb=(b) \subsetneqq R$。由 Dedekind 环性质知$(b)=M_1^{n_1}\cdots M_k^{n_k}$，$M_i \in \mathrm{Max}R$，$i=1,\cdots,k$。因此

$$R/(b) \simeq R/M_1^{n_1} \oplus \cdots \oplus R/M_k^{n_k}\ (\text{由中国剩余定理})。$$

但作为加法 Abel 群，有有限长次正规列(subnormal series)

$$1 \lhd M_i^{n_i-1}/M_i^{n_i} \lhd \cdots M_i/M_i^{n_i} \lhd R/M_i^{n_i}, \quad i=1,\cdots,k。$$

我们先来证明每一个次正规列的各因子（相邻者的商群）都是同构的。为此先证

引理 7.2 设 R 为 Dedekind 环，A,B 为 R 的非零理想，则

(1) 必有 R 的理想 C 使 $B+C=R$ 且 $AC=(\alpha)$为 R 的主理想；

(2) $R/B \simeq A/AB$。

证 (1) 由 R 为 Dedekind 环知可设

$$A = P_1^{a_1}\cdots P_n^{a_n}, \qquad B = P_1^{b_1}\cdots P_n^{b_n},$$

其中 $P_j \in \mathrm{Max}R$，$a_j, b_j \geqslant 0$。由 Dedekind 环理想的惟一分解性知 $P_i^{a_i} \neq P_i^{a_i+1}$，于是必有 $0 \neq \alpha_i \in P_i^{a_i} \setminus P_i^{a_i+1}$，$i=1,\cdots,n$，但 $P_i^{a_i+1}+P_j^{a_j+1}=R$，$\forall i \neq j$。（否则必有 $M \in \mathrm{Max}R$ 使 $M \supset P_i^{a_i+1}+P_j^{a_j+1}$，于是由 $M \in \mathrm{Max}R \subset \mathrm{Spec}R$ 知 P_i、P_j 都在 M 内，这不可能）。因此由中国剩余定理知，必有 $\alpha \in R$ 使

$$\alpha \equiv \alpha_i (\bmod P_i^{a_i+1})(\text{因此 } \alpha \equiv \alpha_i (\bmod P_i^{a_i})), \qquad i=1,\cdots,n$$

显然，$\alpha \in P_i^{a_i} \setminus P_i^{a_i+1}$，$i=1,\cdots,n$。由此知 $\alpha \in \bigcap_{i=1}^{n} P_i^{a_i} = P_1^{a_1}\cdots P_n^{a_n}=A$。于是

$$(\alpha)+AB \subseteq A$$

因此

$$(\alpha)+AB = P_1^{c_1}\cdots P_n^{c_n}, \qquad c_i \geqslant a_i,\ i=1,\cdots,n$$

但由 $\alpha\notin P_i^{a_i-1}$ 知 $c_i=a_i, i=1,\cdots,n$,即$(\alpha)+AB=A$,而由 $\alpha\in A$,用理想的因子分解惟一性又知,必有 $C\lhd R$ 使$(\alpha)=AC$。于是

$$AC + AB = A$$

最后由 Dedekind 环的另一(特征)性质——一切非零理想都可逆,两边乘以 A 的逆理想即得 $B+C=R$。

(2) 在(1)的基础上作加群同态

$$\pi: R \to A/AB$$
$$r \mapsto r\alpha + AB$$

由$(\alpha)+AB=A$ 知,π 为满同态。

令 $x\in\mathrm{Ker}\pi$,即 $x\alpha\in AB$,于是 $x\alpha C\subseteq ABC=ACB=(\alpha)B=\alpha RB=\alpha B$,由此知 $xC\subseteq B$. 再由 $B+C=R$ 知,有 $b_1\in B, c_1\in C$ 使 $b_1+c_1=1$,于是 $x=x\cdot 1=xb_1+xc_1\in B$,即 $\mathrm{Ker}\pi\subseteq B$。

反之,任取 $b_2\in B$,则 $\pi(b_2)=b_2\alpha+AB \xlongequal[(\alpha\in A)]{} AB$,即 $b_2\in\mathrm{Ker}\pi$,从而 $B\subseteq\mathrm{Ker}\pi$,故 $\mathrm{Ker}\pi=B$,因而 $R/B\simeq A/AB$,引理证毕。

再接着证明命题 7.2,事实上取上引理之(2)中的 $A=M_i^m, B=M_i$ 即得

$$R/M_i \simeq M_i^m/M_i^{m+1}, \qquad i = 1,\cdots,k$$

于是,前述之次正规列各因子作为加群都同构于 R/M_i。因此

$$|R/M_i^{n_i}| = |R/M_i|^{n_i} < \infty$$

从而

$$|R/(b)| = |R/M_1|^{n_1}\cdots|R/M_k|^{n_k} < \infty$$

由此知$(R/(b))^{\cdot}$ 为有限(乘法)群。

由$(a,b)\in U_2(R)$知必有 $x,y\in R$ 使 $ax+by=1$。于是 $\bar{a}$ 在 $R/(b)$中可逆,即 $\bar{a}\in(R/(b))^{\cdot}$,从而由$(R/(b))^{\cdot}$ 的有限性知 $\mathrm{ord}\bar{a}=s<\infty$。因此,$a^s\equiv 1(\mathrm{mod}\ b)$,即有 $r\in R$ 使 $a^s=1+rb$。由此知

$$[a\ b]^s = [a^s\ b] = [1 + rb\ b] = [1\ b] = 1。$$ □

由上面证明的末段,我们已得到更好的如下结果:

命题 7.3　设 $R\in\mathcal{C}\mathrm{Ring}$,且对 $\forall\,0\neq r\in R$, $|R/(r)|<\infty$,则 $\forall\,(a,b)\in U_2(R)$,$[a\ b]$都是挠元素,因此 Mennicke 符号生成的 $SK_1(R)$的子群为挠群。若又有 $\mathrm{Sr}(R)=2$,则 $SK_1(R)$为挠群。

下面来研究代数数域 F 中代数整元环 O_F(§23 将证明 O_F 为 Dedekind 环),这是最常用的一类 Dedekind 环(比如可见[Ireland, 1982])。我们来证明 O_F 正好满足命题 7.2 的条件,以说明命题 7.2 有较广的应用背景。

为研究上述的 O_F，再证明两条引理。

引理 7.3 设 O_F 为代数数域 F 中的代数整元环，$0\neq A\lhd O_F$，$\alpha_1,\cdots,\alpha_n$ 为 F 在 $\mathbb{Q}$ 上的基且 $\alpha_j\in A$，$j=1,\cdots,n$，使

$$|\Delta(\alpha_1,\cdots,\alpha_n)|=\min\{|\Delta(\beta_1,\cdots,\beta_n)|\mid\beta_j\in A,$$
$$j=1,\cdots,n\text{ 且 }\beta_1,\cdots,\beta_n\text{ 为 }F\text{ 在 }\mathbb{Q}\text{ 上之基}\},$$

则 $A=\mathbb{Z}\alpha_1+\cdots+\mathbb{Z}\alpha_n$，其中 $\Delta(\alpha_1,\cdots,\alpha_n)=\det(\mathrm{Tr}(\alpha_i\alpha_j))$，为 $\alpha_1,\cdots,\alpha_n$ 的判别式，而 $\mathrm{Tr}(\alpha)$ 表示代数整数 α 的迹(trace)，即 α 的极小多项式(必为首一的) $f(x)\in\mathbb{Z}[x]$ 的各根之和。称 $\alpha_1,\cdots,\alpha_n$ 为 A 的**整基**(integral basis)。

证 反设有 $\alpha\in A$，$\alpha=a_1\alpha_1+\cdots+a_n\alpha_n$，$a_j\in\mathbb{Q}$，$j=1,\cdots,n$ 不全为整数。不妨设 $a_1\notin\mathbb{Z}$，于是 $a_1=m+\theta$，$m\in\mathbb{Z}$，$0<\theta<1$。

令 $\beta_1=\alpha-m\alpha_1$，$\beta_j=\alpha_j$，$j=2,\cdots,n$，则 $\beta_1,\cdots,\beta_n\in A$ 且仍为 F 在 $\mathbb{Q}$ 上的基。但

$$\beta_1=\alpha-m\alpha_1=\theta\alpha_1+a_2\alpha_2+\cdots+a_n\alpha_n$$

由 $\alpha_1,\cdots,\alpha_n$ 到 $\beta_1,\cdots,\beta_n$ 的演化矩阵为

$$P=\begin{pmatrix}\theta & a_2 & \cdots & a_n\\ & 1 & & \\ & & \ddots & \\ & & & 1\end{pmatrix}\equiv(p_{ij})$$

注意 $\beta_i\beta_k=\sum_j\sum_l p_{ij}p_{kl}\alpha_j\alpha_l$，令 $A_1=(\mathrm{Tr}(\beta_i\beta_k))$，$A_2=(\mathrm{Tr}(\alpha_j\alpha_l))$，则

$$A_1=P'A_2P$$

于是

$$\Delta(\beta_1,\cdots,\beta_n)=(\det P)^2\Delta(\alpha_1,\cdots,\alpha_n)=\theta^2\Delta(\alpha_1,\cdots,\alpha_n)$$

由于 $0<\theta<1$，这与 $|\Delta(\alpha_1,\cdots,\alpha_n)|$ 的最小性矛盾，故 $A=\mathbb{Z}\alpha_1+\cdots+\mathbb{Z}\alpha_n$。□

引理 7.4 设 O_F 为代数数域 F 中的代数整元环，$0\neq A\lhd O_F$，则 $A\cap\mathbb{Z}\neq0$ 且 $|O_F/A|<\infty$。因此 O_F/M 为有限域，$\forall M\in\mathrm{Max}O_F$(常称 $|O_F/A|$ 为 A 的范数(norm)，记为 $\|A\|$)。

证 令 F 在 $\mathbb{Q}$ 上基为 $\beta_1,\cdots,\beta_n$，$\forall\beta\in F$，必有 $a_j\in\mathbb{Z}$，$a_0\neq0$ 使

$$a_0\beta^m+a_1\beta^{m-1}+\cdots+a_m=0,\qquad m\leqslant n,$$

以 a_0^{m-1} 乘上式两端得

$$(a_0\beta)^m+a_1(a_0\beta)^{m-1}+\cdots+a_ma_0^{m-1}=0$$

因此 $a_0\beta\in O_F$。由此知必有 $b_j\in\mathbb{Z}$ 使 $b_j\beta_j\in O_F$，记 $b=b_1\cdots b_n$ 则 $b\beta_j\in O_F$，$j=1,\cdots,n$。任取 $0\neq a\in A$，则 $ab\beta_1,\cdots,ab\beta_n\in A$，且易验知它们仍为 F 在 $\mathbb{Q}$ 上的基，记为 $\alpha_j=ab\beta_j$，$j=1,\cdots,n$。但 $0\neq a\in A\subseteq O_F$，于是又有 $c_j\in\mathbb{Z}$ 使

$$a^t + c_1 a^{t-1} + \cdots + c_t = 0, \qquad c_t \neq 0$$

由此知

$$0 \neq c_t = -a^t - c_1 a^{t-1} - \cdots - c_1 a \in A \cap \mathbb{Z}$$

因此 $A \cap \mathbb{Z} \neq 0$。于是上面的 a 可取自 $A \cap \mathbb{Z}$ 中,且可设 $a>0$。

作加群同态

$$\pi: O_F/(a) \to O_F/A$$
$$r+(a) \mapsto r+A$$

易看出 π 为满同态。因此只要证明 $|O_F/(a)|<\infty$ 即可。

注意对 $\forall \alpha \in O_F$, $\mathrm{Tr}(\alpha) \in \mathbb{Z}$,可知 $\Delta(\alpha_1,\cdots,\alpha_n) \in \mathbb{Z}$,因此可令上述的 $\alpha_1,\cdots,\alpha_n$ 为 O_F 内 F 在 $\mathbb{Q}$ 上之基中判别式绝对值最小者。于是由引理 7.3 知

$$O_F = \mathbb{Z}\alpha_1 + \cdots + \mathbb{Z}\alpha_n$$

任取 $\alpha \in O_F$,则 $\alpha = c_1\alpha_1 + \cdots + c_n\alpha_n$, $c_i \in \mathbb{Z}$, $i=1,\cdots,n$,作 $\mathbb{Z}$ 中的带余除法:

$$c_i = q_i a + r_i, \qquad 0 \leqslant r_i < a,$$

则 α 在 $O_F/(a)$ 中的象 $\bar{\alpha} \equiv \Sigma r_i (\mathrm{mod}\ a)\alpha_i$。于是由 $a \in A \cap \mathbb{Z}$, $a>0$ 即知

$$|O_F/(a)| \leqslant a^n < \infty$$ □

由命题 7.2,引理 7.4 立得

推论 7.2　设 O_F 为代数数域 F 中的代数整元环,则 $SK_1(O_F)$ 为挠群。

注②　事实上由命题 7.2 之证已看出:对 Dedekind 环 R 中的任一非零理想 A, $|R/A|<\infty \Leftrightarrow |R/M|<\infty$, $\forall M \in \mathrm{Max}R$。$\Leftrightarrow R/M$ 为有限域, $\forall M \in \mathrm{Max}R$。

注③　正如§5 注①所述,1967 年,H. Bass, J. Milnor 与 J. P. Serre 已证出彻底改进推论 7.2 的结果。他们的结果是:设 R 为 Dedekind 环,其商域为 $\mathbb{Q}$ 的有限次扩张(即 $[Q(R):\mathbb{Q}]<\infty$(如 $R=O_F$)),则 $K_1(R) \simeq R^\cdot$,因此 $SK_1(O_F)=1$(见[Milnor,1971]的§16)。但证明中要用到代数拓扑的一些工具。他们还同时证明了:对单位圆的坐标环

$$R = \mathbb{R}[x,y]/(x^2+y^2-1)$$

(当然是 Dedekind 环),

$$\begin{pmatrix} x & y \\ -y & x \end{pmatrix} \in SL_2(R)$$

对应的 Mennicke 符号 $[x\ y] \neq 1$ 且为 2 阶元。从而说明 Mennicke 符号及 Dedekind 环的 SK_1 群可以是不平凡的。

由定理 7.1′知,对 Dedekind 环 R 的 K_1 群,使用 Mennicke 符号处理了 SK_1 群之后,了解一下 $R^\cdot$ 的结构是有益的,尤其是对代数数域 F 中的代数

整元环 O_F(已知 $SK_1(O_F)=1$)。下面列出著名的 Dirichlet 单位定理供读者参考,欲知其证法的读者,可参看[Rosenberg,1994]。

Dirichlet 单位(数)(unit)定理(1846) 设 O_F 为代数数域 F 中的代数整元环,则 $O_F^{\cdot}$ 是有限生成的(乘法 Abel 群),其挠子群 W 为 F 中的单位根生成的有限循环群(称为 F 的单位根群,也常记为(ξ))。其无挠部分 $O_F^{\cdot}/W$ 为秩等于 r_1+r_2-1 的自由 Abel 群,其中 $r_1+2r_2=n=[F:\mathbb{Q}]$,$r_1$ 为 F 到$\mathbb{R}$ 的不同的嵌入数($F=\mathbb{Q}(\alpha)$,α 的实共轭个数),r_2 为 F 到$\mathbb{C}$ 象不在$\mathbb{R}$ 中的不同的嵌入共轭对的个数(α 的虚共轭对个数)。特别地,$|O_F^{\cdot}|=\infty\Leftrightarrow F\neq\mathbb{Q}$ 且 F 不是虚二次域。

事实上,对虚次域 $F=\mathbb{Q}(\sqrt{d})$,$d<0$,记 $U_d=O_F^{\cdot}$,则

$U_{-1}=\{\pm1,\pm i\}\simeq\mathbb{Z}_4$,

$U_{-3}=\{\pm1,\pm w,\pm w^2\}\simeq\mathbb{Z}_6$,其中 $w=(-1+\sqrt{-3})/2$,

$U_d=\{\pm1\}\simeq\mathbb{Z}_2$, $\forall d<-3$ 或 $d=-2$。

对实二次域 $F=\mathbb{Q}(\sqrt{d})$,$d>0$,必有 $u\in O_F$,$u>1$ 使 $O_F^{\cdot}=\{\pm u^m,m\in\mathbb{Z}\}$(参看[Ireland,1982]的 Ch. 13)。

比如,$F=\mathbb{Q}(\sqrt{-1})$时,$n=2$,$r_1=0$,$r_2=1$,$r_1+r_2-1=0$。

$O_F=\mathbb{Z}[\sqrt{-1}]$,

$O_F^{\cdot}=\{\pm1,\pm i\}=W(\simeq C_4$(四阶循环群)$\simeq\mathbb{Z}_4)$,

$F=\mathbb{Q}(\sqrt{2})$时,$n=2$,$r_1=2$,$r_2=0$,$r_1+r_2-1=1$,

$O_F=\mathbb{Z}[\sqrt{2}]$,

$O_F^{\cdot}=\{\pm(1+\sqrt{2})^n,n\geqslant0\}$,$W=\{\pm1\}(\simeq C_2\simeq\mathbb{Z}_2)$,

$O_F^{\cdot}/W\simeq\mathbb{Z}$(无限循环群,即秩为 1 的自由 Abel 群)。

因此 $K_1(\mathbb{Z}[\sqrt{2}])\simeq\mathbb{Z}_2\oplus\mathbb{Z}$。

由 Dirichlet 单位定理可得下述结果:

定理 7.3 设 F 为代数数域,O_F 为 F 中的代数整元环,则

$$K_1(O_F)\simeq O_F^{\cdot}\simeq W\oplus\mathbb{Z}^{r_1+r_2-1}.$$

其中 W 为 F 的单位根群,是一个有限循环群。

§8 Dieudonné 行列式与局部环的 K_1 群

由于域上的行列式可照搬到交换环上,在上两节中我们对交换环中的

GE 环(广义 Euclid 环),局部环、半局部环以及 Sr1 环(稳定环),代数整元环 O_F 环等都得出完美的结果。即当 R 为交换环中的这些环时,$K_1(R)\simeq R^\cdot$,但对非交换环 R,即使 R 是除环、局部环,也只得出 $R^{\cdot ab}$ 到 $K_1(R)$ 有满同态这一结果。由此可见,研究行列式可向哪些非交换环推广,是不容回避的一个有意义的问题。本节的主要目的就是通过这一问题的研究,对除环,乃至非交换局部环 R 的 K_1 群,得到 $K_1(R)\simeq R^{\cdot ab}$ 这种令人满意的结果。

在§6 中,我们已经知道,$R\in GE \Leftrightarrow \forall n, A\in GL_n(R), A=ED$,其中 $E\in E_n(R)$,$D=\mathrm{diag}(d,1,\cdots,1)$,$d\in R^\cdot$。但 d 是否惟一确定(或至少在 mod $R^{\cdot ab}$ 意义下),尚属未知,当然,当 R 又为交换环时这个 d 即为 A 的行列式,是由 A 惟一确定的。事实上交换环上矩阵的行列式的本质可见于如下易于直接验证的命题。

命题 8.1　设 $R\in$ CRing,则群同态 $\det: GL_n(R)\twoheadrightarrow R^\cdot$ 满足:

(a) $E_n(R)\subseteq \mathrm{Ker}\det = SL_n(R)$;

(b) $\det\mathrm{diag}(a_1,\cdots,a_n)=a_1\cdots a_n$, $\forall a_j\in R^\cdot$;

(c)

$$
\begin{array}{ccc}
GL_n(R) & \xrightarrow{\ i_1\ } & GL_{n+1}(R) \\
 & \searrow^{\det} \quad \swarrow_{\det} & \\
 & R^\cdot &
\end{array}
$$

为交换图。

对一般的 $R\in$ Ring,则有下面的交换图:

$$
\begin{array}{ccc}
GL_n(R) & \xrightarrow{\ i\ } & GL_{n+1}(R) \\
 & \searrow^{\pi i} \quad \swarrow_{\pi} & \\
 & K_1(R) &
\end{array}
$$

其中的 πi 模拟着命题 8.1(c)中的 det,常称为 $GL_n(R)$ 的 **Whitehead 行列式**,当 $R\in GE_n$ 时,这种模拟更加逼真。但这种行列式不便于计算(因为 $K_1(R)$ 尚需计算),且行列式性质显示得不多。为研究一般非交换环 R 上 $GL_n(R)$ 的行列式,先证

引理 8.1　设 $R\in$ Ring,则

(1) $R\in GE_n$ 且 $n\geqslant 2$ 时,$GL_n(R)'\equiv[GL_n(R),GL_n(R)]\subseteq E_n(R)$;

(2) $n\geqslant 3$ 时 $GL_n(R)'\supseteq E_n(R)$;

(3) $R\in GE_n$ 且 $n\geqslant 3$ 时,$GL_n(R)'=E_n(R)$;

(4) $R=R^{\cdot}+R^{\cdot}$(如 R 为基数$\geqslant 3$ 的除环,见 §9)时,$\mathrm{GL}_2(R)'\supseteq \mathrm{E}_2(R)$,因此若 R 又满足 $R\in \mathrm{GE}_n$,$\forall n\geqslant 2$,则必有 $\mathrm{GL}_n(R)'=\mathrm{E}_n(R)$,$\forall n\geqslant 2$。

证 (1) 由 $R\in \mathrm{GE}_n$ 知,$\forall A_j\in \mathrm{GL}_n(R)$,$A_j=B_jD_j$,$B_j\in \mathrm{E}_n(R)$,$D_j=\mathrm{diag}(d_j,1,\cdots,1)$为可逆对角阵,$j=1,2$。于是

$$\begin{aligned}[A_1,A_2]&= B_1D_1B_2D_2D_1^{-1}B_1^{-1}D_2^{-1}B_2^{-1}\\ &=\{B_1(D_1B_2D_1^{-1})((D_1D_2D_1^{-1})B_1^{-1}(D_1D_2D_1^{-1})^{-1})\\ &\quad((D_1D_2D_1^{-1}D_2^{-1})B_2^{-1}(D_1D_2D_1^{-1}D_2^{-1})^{-1})\}D_1D_2D_1^{-1}D_2^{-1}\end{aligned}$$

注意对可逆对角阵 $D=\mathrm{diag}(a_1,a_2,\cdots,a_n)$(参见 §6 命题 6.1 之证中的(*)),

$$De_{ij}^{x}D^{-1}=e_{ij}^{a_ixa_j^{-1}},$$

于是前式右端$\{\cdots\}\in \mathrm{E}_n(R)$。又由推论 5.1 知

$$D_1D_2D_1^{-1}D_2^{-1}=[D_1,D_2]=\mathrm{diag}([d_1,d_2],1,\cdots,1)\in \mathrm{E}_n(R)$$

故$[A_1,A_2]\in \mathrm{E}_n(R)$,因此由 A_1,A_2 的任意性知 $\mathrm{GL}_n(R)'\subset \mathrm{E}_n(R)$。

(2) 事实上,由命题 5.1 知 $n\geqslant 3$ 时 $\mathrm{E}_n(R)=\mathrm{E}_n(R)'$,于是

$$\mathrm{E}_n(R)=\mathrm{E}_n(R)'\subseteq \mathrm{GL}_n(R)'$$

(3) 由(1),(2)即得。

(4) 由 $R=R^{\cdot}+R^{\cdot}$ 知,$\forall x\in R$,可记 $x=a+b$,$a,b\in R^{\cdot}$,下证有 $A,B\in \mathrm{GL}_2(R)$使

$$e_{12}^{x}=\begin{pmatrix}1 & a+b\\ & 1\end{pmatrix}=[A,B]$$

为此只需证 e_{12}^{x}可经 4 次对应换位子的广义初等行变换(对应广义初等矩阵,包括 $u(i)$,$u\in R^{\cdot}$,形的行变换)变成 I_2(由于 e_{12}^{x}的第 2 行无需再变,尽量只变第 1 行)。

$$e_{12}^{x}=\begin{pmatrix}1 & a+b\\ & 1\end{pmatrix}\xrightarrow[(1)-b(2)]{}\begin{pmatrix}1 & a\\ & 1\end{pmatrix}\xrightarrow[-ba^{-1}(1)]{}\begin{pmatrix}-ba^{-1} & -b\\ & 1\end{pmatrix}$$

$$\xrightarrow[(1)+b(2)]{}\begin{pmatrix}-ba^{-1} & \\ & 1\end{pmatrix}\xrightarrow[-ab^{-1}(1)]{}I_2$$

故 $e_{12}^{x}\in \mathrm{GL}_2(R)'$。同理 $e_{21}^{x}\in \mathrm{GL}_2(R)'$故 $\mathrm{E}_2(R)\subseteq \mathrm{GL}_2(R)'$。 □

命题 8.2 设 $R\in \mathrm{GE}_n$,$R^{\cdot}$ 不是交换的(即有 $a,b\in R^{\cdot}$ 使 $ab\neq ba$)(比如四元数体$\mathbb{H}$),则命题 8.1 中的群同态 $\det:\mathrm{GL}_n(R)\to R^{\cdot}$ 不存在。

证 反设 det 存在,且有性质(a),(b),(c),由(b)知 det 为满同态。由(a)知 $\mathrm{E}_n(R)\subseteq \mathrm{Ker}\det$,但由引理 8.1(1)知,$n\geqslant 2$ 时 $\mathrm{GL}_n(R)'\subseteq \mathrm{E}_n(R)$,于是 $\mathrm{GL}_n(R)'\subseteq \mathrm{Ker}\det$。由此知有从 Abel 群 $\mathrm{GL}_n(R)^{ab}$ 到 $R^{\cdot}$ 的满同态

$$\mathrm{GL}_n(R)^{ab} \cong \mathrm{GL}_n(R)/\mathrm{GL}_n(R)' \underset{\det}{\twoheadrightarrow} R^{\cdot}$$

因此 $R^{\cdot} \in \mathcal{A}\mathrm{G}$ 与题设矛盾，故 det 不存在。 □

命题 8.2 又一次更清楚地指出：域上行列式不能照搬到非交换环（甚至不能照搬到除环）。为作这方面的推广，起码要将 $R^{\cdot}$ 改为 $R^{\cdot ab}=R^{\cdot}/[R^{\cdot}, R^{\cdot}]$，由此引出著名数学家 J. Dieudonné 为研究除环上典型群给出的一种广义行列式。

定义 8.1　设 $R\in \mathcal{R}\mathrm{ing}$，$\pi: R^{\cdot} \to R^{\cdot ab}$ 为标准群同态，$\bar{a}=\pi(a)$，$\forall a\in R^{\cdot}$。若群同态 $\det: \mathrm{GL}_n(R)\to R^{\cdot ab}$ 满足：

(a) $\mathrm{E}_n(R)\subseteq \mathrm{Ker}\det$；

(b) $\det \mathrm{diag}(a_1, \cdots, a_n)=\overline{a_1\cdots a_n}$，$\forall a_j\in R^{\cdot}$；

(c)
$$\begin{array}{ccc} \mathrm{GL}_n(R) & \xrightarrow{i_1} & \mathrm{GL}_{n+1}(R) \\ {\scriptstyle\det}\searrow & & \swarrow{\scriptstyle\det} \\ & R^{\cdot ab} & \end{array}$$

为交换图，则称 det 为（$\mathrm{GL}_n(R)$ 上或 $\mathrm{GL}(R)$ 上的）**Dieudonné 行列式（映射）（D-行列式）**。

容易看出 $R\in \mathcal{C}\mathrm{Ring}$ 时，对 $\mathrm{GL}_n(R)$ 通常的行列式即 Dieudonné 行列式。

显然 det 可开拓为同态：$\mathrm{GL}(R)\to R^{\cdot ab}$，又由§6 知，对 $R\in \mathrm{GE}_n$，$\forall A\in \mathrm{GL}_n(R)$，$A=BD$，其中 $B\in \mathrm{E}_n(R)$，$D=\mathrm{diag}(d, 1, \cdots, 1)$，$d\in R^{\cdot}$，因此 $A\equiv D(\mathrm{mod}\,\mathrm{E}_n(R))$。由此可知对 GE 环（如局部环与除环），Dieudonné 行列式若存在，则必惟一。

注①　Dieudonné 行列式也可开拓为对 $R^{n\times n}$ 使用，即规定 $A\in R^{n\times n}\setminus \mathrm{GL}_n(R)$ 时 $\mathrm{Det}A=0$，$R^{\cdot ab}$ 开拓为 $R^{\cdot ab}\cup\{0\}$，$\mathrm{Det}|_{\mathrm{GL}_n(R)}=\det: \mathrm{GL}_n(R)\to R^{\cdot ab}$。显然 Det 为保持乘法的映射（不是群同态，因为 $R^{\cdot ab}\cup\{0\}$ 不是群，它事实上是半群同态）。

为证明：对除环乃至局部环上的矩阵，Dieudonné 行列式存在，先证下述引理。

引理 8.2　设 R 为除环，则注①中开拓后定义的保持乘法映射 Det，作为映射，等价于满足下述条件的映射 $\mathrm{Det}: R^{n\times n}\to R^{\cdot ab}\cup\{0\}$，（（1°），（2°）中的行变换也可改为列变换）。

（1°）$\forall a\in R, A\in R^{n\times n}$，若 $A\xrightarrow[a(i)]{} B$，则 $\mathrm{Det}B=\bar{a}\mathrm{Det}A$，其中 $a\notin R^{\cdot}$ 时规定 $\bar{a}=0$；

（2°）$\forall a\in R, A\in R^{n\times n}$，若 $A\xrightarrow[(i)+a(j)]{} B$，则 $\mathrm{Det}B=\mathrm{Det}A$；

(3°) $\mathrm{Det}I_n=\bar{1}$。

因此,(未经如上开拓的)Dieudonné 行列式对除环而言,即满足(1°)(其中 $a\in R^{\cdot}$, $A\in \mathrm{GL}_n(R)$),(2°)(其中 $A\in\mathrm{GL}_n(R)$),与(3°)的群同态 $\det:\mathrm{GL}_n(R)\to R^{\cdot ab}$。

证 1. 先证(保持乘法的)映射 Det 满足(1°),(2°),(3°)(不用除环条件!)。

(1°) 由 $A\xrightarrow[a(i)]{}B$ 知,$B=\mathrm{diag}(1,\cdots,1,a,1,\cdots,1)A$,又由 Det 保持乘法知,

$$\mathrm{Det}B=\mathrm{Det}\ \mathrm{diag}(1,\cdots,1,a,1,\cdots,1)\mathrm{Det}A$$
$$\overset{}{\underset{(\bar{b})}{=\!=}}\bar{a}\mathrm{Det}A,a\notin R^{\cdot}\text{ 时 }\bar{a}=0$$

(2°) 由 $A\xrightarrow[(i)+a(j)]{}B$ 知,$B=e_{ij}^{a}A$,于是由 Det 保持乘法知

$$\mathrm{Det}B=\mathrm{Det}e_{ij}^{a}\mathrm{Det}A\underset{(a)}{=\!=}\bar{1}\mathrm{Det}A=\mathrm{Det}A$$

(3°) 由($\bar{\mathrm{b}}$)即得。

2. 证明满足(1°),(2°),(3°)的映射 $\mathrm{Det}:R^{n\times n}\to R^{\cdot ab}\cup\{0\}$ 保持乘法,且限制于 $\mathrm{GL}_n(R)$ 上为满足(a),($\bar{\mathrm{b}}$),(c)的同态 $\det:\mathrm{GL}_n(R)\to R^{\cdot ab}$。

先证 Det 满足(1°),(2°),(3°)时必保持乘法。由于 R 为除环,对 $\forall C\in R^{n\times n}$ 都有惟一的秩 rankC(行秩,列秩的公共值)且 $\mathrm{rank}C<n\Leftrightarrow C\notin\mathrm{GL}_n(R)$,因此,若 $A\in R^{n\times n}\backslash\mathrm{GL}_n(R)$,$B\in R^{n\times n}$,则 $\mathrm{rank}A<n$ 且 $\mathrm{Det}A=0$。又

$$\mathrm{rank}(AB)\leqslant\min(\mathrm{rank}A,\mathrm{rank}B)<n,$$

于是 $AB\notin\mathrm{GL}_n(R)$,$\mathrm{Det}AB=0=\mathrm{Det}A\cdot\mathrm{Det}B$。若 $A\in\mathrm{GL}_n(R)$,由 $R\in\mathrm{GE}$ 知,$A=ED$,其中 $E\in\mathrm{E}_n(R)$,$D=\mathrm{diag}(d,1,\cdots,1)$,$d\in R^{\cdot}$。用(2°)得

$$\mathrm{Det}A=\mathrm{Det}D\underset{(1^\circ)}{=\!=}\bar{d}$$

若 $B\in R^{n\times n}$,则 $AB=EDB$。同理知

$$\mathrm{Det}(AB)\overset{(2^\circ)}{=\!=}\mathrm{Det}(DB)\overset{(1^\circ)}{=\!=}\bar{d}\mathrm{Det}B=\mathrm{Det}A\mathrm{Det}B$$

再来证 Det 限制于 $\mathrm{GL}_n(R)$ 上为满足(a),($\bar{\mathrm{b}}$),(c)的映射。事实上,由 Det 保持乘法,从(2°),(3°)得(a)是显见的。注意到 $R\in\mathrm{GE}$,$\forall A\in\mathrm{GL}_n(R)$,$A=ED$,$E\in\mathrm{E}_n(R)$,$D=\mathrm{diag}(d,1,\cdots,1)$,在 $\mathrm{GL}_{n+1}(R)$ 中则有

$$\begin{pmatrix}A&\\&1\end{pmatrix}=\begin{pmatrix}E&\\&1\end{pmatrix}\begin{pmatrix}D&\\&1\end{pmatrix}$$

因此(c)也是显见的。下证($\bar{\mathrm{b}}$),这只需注意到

$$\mathrm{diag}(a_1,\cdots,a_n)=(\mathrm{diag}(a_1,1,\cdots,1)I_n)$$
$$\cdots(\mathrm{diag}(1,\cdots,a_j,\cdots,1)I_n)\cdots(\mathrm{diag}(1,\cdots,a_n)I_n)$$

用 Det 的保持乘法性质及(1°),(3°)即得

$$\mathrm{Det}\ \mathrm{diag}(a_1,\cdots,a_n) = \bar{a}_1\cdots\bar{a}_j\cdots\bar{a}_n = \overline{a_1\cdots a_n}$$

即($\bar{\mathrm{b}}$)成立。 □

注意到上面证明的前一部分未用到"R 为除环"这一条件,即得下述推论。

推论 8.1 设 $R\in$ Ring,若 Dieudonné 行列式存在,则必满足引理 8.2 中的(1°),(2°),(3°)。

对 GE_n 环(比如 Euclid 环,局部环,半局部环)还可得出:当引理 8.2 中的映射 Det 存在时,限制于 $\mathrm{GL}_n(R)$上必然还具备保持乘法的性质以及通常行列式具有的关于交换行与转置的性质。注意,这里的 $A=(a_{ij})\in R^{n\times n}$ 的转置矩阵 $A^T=(a_{ji})$是被定义为 R 的反环 R^o 上的 $n\times n$ 矩阵(但正如过去已用过的,为方便起见,将列向量写成行的形式时,也常用"T"表转置)。容易看出:$(AB)^T=B^TA^T$,且 $R\in\mathrm{GE}_n\Leftrightarrow R^o\in\mathrm{GE}_n$。事实上,矩阵的转置给出了 R 与 R^o 上 $n\times n$ 矩阵环的反同构($R\in$ CRing 时为同构),这个反同构保持着 GL_n,E_n 等乘法群的对应。现在来证下述结果。

命题 8.3 设 $R\in\mathrm{GE}_n$ 且引理 8.2 中的 Det 存在,则 $\mathrm{GL}_n(R)$上的 Dieudonné 行列式 det 存在且惟一,同时有下述性质:

(4°) $\forall A,B\in\mathrm{GL}_n(R)$,$\det(AB)=\det A\cdot\det B$;

(5°) $\forall A\in\mathrm{GL}_n(R)$,若 $A\xrightarrow[(i)\leftrightarrow(j)]{}A_1$,则 $\det A_1=(-\bar{1})\det A=-\det A$;

(6°) $\forall A\in\mathrm{GL}_n(R)$,$\det A^T=\det A$。

证 先证 Det 存在时,$\mathrm{GL}_n(R)$上的 Dieudonné 行列式 $\det=\mathrm{Det}|_{\mathrm{GL}_n(R)}$ 惟一。事实上,由 $R\in\mathrm{GE}_n$ 知,$\forall A\in\mathrm{GL}_n(R)$,$A=ED$,$E\in\mathrm{E}_n(R)$,$D=\mathrm{diag}(d,1,\cdots,1)$,$d\in R^*$,因此 A 可看作是单位矩阵 I_n 经 $d(1)$,及若干次$(i)+b(j)$形初等变换而得。于是由(1°),(2°),(3°)知 $\bar{d}=\det A$。若又有 $A=E_1D_1$,$E_1\in\mathrm{E}_n(R)$,$D_1=\mathrm{diag}(d_1,1,\cdots,1)$,$d_1\in R^*$,则由 $ED=E_1D_1$ 知 $E_1^{-1}ED=D_1$。再由(1°),(2°),(3°)又知 $\det D=\bar{d}=\bar{d}_1=\det D_1$,即 $\det(ED)=\det(E_1D_1)$,因此 $\det A$ 是惟一确定的(与上述分解无关)。

再来证 det 满足(4°),(5°),(6°)。

由(2°),$\forall B\in\mathrm{GL}_n(R)$,$A=ED$,$E\in\mathrm{E}_n(R)$,$D=\mathrm{diag}(d,1,\cdots,1)$,$d\in R^*$,

$$\det(AB)=\det((E^{-1}A)B)=\det(DB)\overset{}{\underset{(1°)}{=\!=}}\bar{d}\det B=\det A\det B。$$

即(4°)成立。

由于$(i)\leftrightarrow(j)$(i,j 行对调)相当于三次初等行变换与一次$(-1)(j)$(参见§5 引理 5.5 与推论 5.1 间的一段),因此$(1°)$,$(2°)\Rightarrow(5°)$是显见的。

最后来证$(6°)$,注意 $\forall A\in GL_n(R)$,$\det A\in R^{\cdot ab}$(Abel 群)。因此,$\forall a\in R^{\cdot}$,$\bar{a}\det A=(\det A)\bar{a}$,$\forall b\in R^{\cdot}$,$\overline{ab}=\overline{ba}$,于是$(1°)$,$(2°)$ 对相应的列变换仍成立。而对 A 作行变换相当于对 A^T 作相应的列变换,于是由 A 的上述分解 $A=ED$ 知,$A^T=DE^T$,$E^T\in E_n(R^o)$。因此 $\det A=\det D$,$\det A^T=\det D$,故 $\det A=\det A^T$,即$(6°)$成立。 □

由此命题知,满足引理 8.2 中$(1°)$,$(2°)$,$(3°)$的 $\mathrm{Det}|_{GL_n(R)}=\det$ 是否存在是一个关键问题。对 GE_n 环类中的局部环(当然包括除环)我们有

命题 8.4 设 R 为局部环(未必为交换环),则引理 8.2 中满足$(1°)$,$(2°)$,$(3°)$的 Det 存在惟一,因此对 $GL_n(R)$的 Dieudonné 行列式 det 存在惟一且满足引理 8.2 中的$(1°)$,$(2°)$,$(3°)$与命题 8.3 中的$(4°)$,$(5°)$,$(6°)$。

证 由 $R\in GE_n$ 与命题 8.3 知,只需证明对 $GL(R)$,det 存在(为书写简单,下面考察列变换且将 $R^{\cdot}$ 的元素从右边乘向量)。为此只需从 $n=1$ 开始归纳地定义 $\det_n:GL_n(R)\to R^{\cdot ab}$,再由对列变换的$(1°)$,$(2°)$与$(3°)$证明

$$\det_{n+m}\begin{pmatrix}A & \\ & I_m\end{pmatrix}=\det_n A,\qquad \forall A\in GL_n(R)$$

从而令 $n\to\infty$即得 $\det:GL(R)\to R^{\cdot ab}$。

$n=1$ 时,定义 $\det_1(a)=\bar{a}$,$\forall a\in R^{\cdot}=GL_1(R)$,当然 $\det_1$ 满足$(1°)$,$(2°)$,$(3°)$。

再设 $k<n$ 时,$\det_k$ 满足$(1°)$,$(2°)$,$(3°)$,来证 $\det_n$ 满足$(1°)$,$(2°)$,$(3°)$。

任取 $A\in GL_n(R)$,记 A 的各列依次为 $A_1,\cdots,A_n$,设 A^{-1} 的第 1 列为$(b_1,\cdots,b_n)^T$。由 $AA^{-1}=I_n$ 知

$$A_1b_1+\cdots+A_nb_n=(1,0,\cdots,0)^T \tag{1}$$

以分块(段)形式记 $A_j=(a_{1j},B_j)^T$。则由此得

$$B_1b_1+\cdots+B_nb_n=0 \tag{2}$$

但 R 为局部环,仿命题 5.1(4)之证知 A^{-1}的任何列不能全为 R 的惟一极大理想 $\mathfrak{m}$ 中的元素。因此其第 1 列中必有 $b_i\in R^{\cdot}=R\backslash\mathfrak{m}$。于是由(2)式得

$$B_1b_1b_i^{-1}+\cdots+B_{i-1}b_{i-1}b_i^{-1}+B_i+B_{i+1}b_{i+1}b_i^{-1}+\cdots+B_nb_nb_i^{-1}=0$$

故由(1)知

$$A\xrightarrow{\widehat{i}+(\sum_{j\neq i}\widehat{j}\,b_j)b_i^{-1}}\begin{pmatrix}a_{11} & \cdots & a_{1,i-1} & b_i^{-1} & a_{1,i+1} & \cdots & a_{1n}\\ B_1 & \cdots & B_{i-1} & 0 & B_{i+1} & \cdots & B_n\end{pmatrix}$$

定义

$$\det_n A = (-1)^{i+1}(\det_{n-1}(B_1\cdots B_{i-1}B_{i+1}\cdots B_n))\bar{b}_i^{-1}$$

只需证 $\det_n$ 满足(1°),(2°),(3°),$\det_n\begin{pmatrix} B & \\ & 1\end{pmatrix}=\det_{n-1}B$,$\forall B\in GL_{n-1}(R)$,

且与 i 的选取无关(即设 $b_i,b_j\in R^{\cdot}$,$i<j$,来证

$$(-1)^i(\det_{n-1}C_i)\bar{b}_i^{-1} = (-1)^j(\det_{n-1}C_j)\bar{b}_j^{-1},$$

其中 $C_i=(B_1\cdots B_{i-1}B_{i+1}\cdots B_n)$,$C_j=(B_1\cdots B_{j-1}B_{j+1}\cdots B_n)$。

事实上,由上述归纳定义知 $\det_n(I_n)=\bar{1}$,从而 $\det_n$ 满足(3°)。又由

$$A\xrightarrow[l\neq k,a\in R]{\hat{l}+\hat{k}a}(A_1\cdots A_{l-1}\,A_l+A_ka\,A_{l+1}\cdots A_n)=Ae_{lk}^a\equiv A'$$

知,$A'^{-1}=(e_{lk}^a)^{-1}A^{-1}=e_{lk}^{-a}A^{-1}$ 的第 1 列为$(b_1,\cdots,b_{l-1},b_l-ab_k,b_{l+1},\cdots,b_n)^T$(注意 A^{-1}的第 1 列为$(b_1,\cdots,b_n)^T$)。

若 $b_t\in R^{\cdot}$,$t\neq k$,则

$$\det_nA'=(-1)^{t+1}(\det_{n-1}(B_1\cdots B_{l-1}\;B_l+B_ka\;B_{l+1}\cdots B_{t-1}\;B_{t+1}\cdots B_n))\bar{b}_t^{-1}$$

由设,$\det_{n-1}$满足(2°)。在后面证明 $\det_n$ 定义与 i 的选取无关后,即知上式右端等于 $\det_nA$,从而此时 $\det_n$ 满足(2°)。

若 $\forall i\neq k$,$b_i\notin R^{\cdot}$,则 $b_k\in R^{\cdot}$,$b_i\in\mathfrak{m}$,$\forall i\neq k$,因此 $b_k-ab_l\notin\mathfrak{m}$,即 $b_k-ab_l\in R^{\cdot}$,此时

$$\det_nA'=(-1)^{k+1}(\det_{n-1}(B_1\cdots B_{k-1}B_{k+1}\cdots B_n))\overline{(b_k-ab_l)}^{-1},$$

$$\det_nA=(-1)^{k+1}(\det_{n-1}(B_1\cdots B_{k-1}B_{k+1}\cdots B_n))\bar{b}_k^{-1}$$

但 $\forall i\neq k$,$b_i\in\mathfrak{m}$,因此 $ab_l\in\mathfrak{m}=J(R)$,于是

$$b_k\equiv b_k-ab_l\,(\mathrm{mod}\ J(R))$$

而 $\tilde{R}=R/J(R)$为除环,当然更是局部环,上面所证明的对 $GL_n(\tilde{R})$均成立,且记 $r\in R$ 在 $\tilde{R}$ 中的(标准)象为 $\tilde{r}$ 后,$\widetilde{J(R)}=0$ 且 $\tilde{b}_k=\widetilde{b_k-ab_l}$。于是由 $ab_l\in J(R)$知,$b_k\equiv b_k-ab_l(\mathrm{mod}[R^{\cdot},R^{\cdot}])$。因此,在下面证明 $\det_n$ 与 i 选取无关后,即知 $\det_nA'=\det_nA$,即 $\det_n$ 满足(2°)。

$\det_n$ 满足(1°)之证可平行于上段关于(2°)的证明。只需将 $\hat{l}+\hat{k}a$ 改为 $\hat{l}a$,$a\in R^{\cdot}$,Ae_{lk}^a改为 $A\,\mathrm{diag}(1,\cdots,1,a,1,\cdots,1)$,$A_l+A_ka$ 改为 A_la,而将 $e_{lk}^{-a}A^{-1}=A'^{-1}$改为 $\mathrm{diag}(1,\cdots,1,a^{-1},1,\cdots,1)A^{-1}=A'^{-1}$,$b_l-ab_k$ 改为 b_la^{-1},B_l+B_ka 改为 B_la,$\det_{n-1}$满足(2°)改为 $\det_{n-1}$满足(1°)。仍分如下两种情况进行论证。

若有 $j\neq i$ 使 $b_j\in R^{\cdot}$，则(在后面证出 $\det_n$ 与 i 选取无关后)有

$$\det_n A' = (-1)^{j+1}(\det_{n-1}(B_1\cdots B_{i-1}B_i a\ B_{i+1}\cdots B_{j-1}B_{j+1}\cdots B_n))\bar{b}_j^{-1}$$
$$= (\det_n A)\bar{a} = \bar{a}\det_n A\text{（注意 } R^{\cdot ab} \text{ 为 Abel 群）。}$$

若 $\forall j\neq i, b_j\in \mathfrak{m}=J(R)$，而 $b_i\in R^{\cdot}$，则(在证出 $\det_n$ 与 i 选取无关后)有

$$\det_n A' = (-1)^{i+1}(\det_{n-1}(B_1\cdots B_{i-1}B_{i+1}\cdots B_n))\overline{b_i a}^{-1}$$
$$\det_n A = (-1)^{i+1}(\det_{n-1}(B_1\cdots B_{i-1}B_{i+1}\cdots B_n))\bar{b}_i^{-1}$$

由 $\overline{b_i a}^{-1}=\bar{a}^{-1}\bar{b}_i^{-1}=\bar{b}_i^{-1}\bar{a}^{-1}$ 即知 $\det_n A'=(\det_n A)\bar{a}=\bar{a}\det_n A$，即 $\det_n$ 满足(1°)。

注意作若干次成对的行对调与列对调($(i)\leftrightarrow(j)$，$\underset{\smile}{i}\leftrightarrow\underset{\smile}{j}$)可使

$$\begin{pmatrix} B & \\ & 1\end{pmatrix}\to\begin{pmatrix} 1 & \\ & B\end{pmatrix},\qquad \forall B\in \mathrm{GL}_{n-1}(R)$$

于是(由(1°)，(2°)，(3°)成立知(5°)成立)

$$\det_n\begin{pmatrix} B & \\ & 1\end{pmatrix}=\det_n\begin{pmatrix} 1 & \\ & B\end{pmatrix}$$
$$\xlongequal[\det_n\text{ 定义}]{} (-1)^{1+1}\det_{n-1}B\cdot\bar{1}=\det_{n-1}B$$

因此

$$\det_{n+m}\begin{pmatrix} A & \\ & I_m\end{pmatrix}=\det_n A,\qquad \forall A\in \mathrm{GL}_n(R)$$

最后来证 $\det_n$ 与 i 的选取无关。为此对前述的 C_i 作 $j-i-1$ 次列对调：$\underset{\smile}{j-1}\leftrightarrow\underset{\smile}{j-2}$，$\underset{\smile}{j-2}\leftrightarrow\underset{\smile}{j-3}\cdots$，$\underset{\smile}{i+1}\leftrightarrow\underset{\smile}{i}$，则使

$$C_i\to(B_1\cdots B_{i-1}B_jB_{i+1}\cdots B_{j-1}B_{j+1}\cdots B_n)\equiv C$$

由 $\det_{n-1}$ 满足(5°)知 $\det_{n-1}C=(-1)^{j-i-1}\det_{n-1}C_i$，而由式(2)又得

$$B_i=-B_jb_jb_i^{-1}+\text{其他列的线性组合。}$$

由 $\det_{n-1}$ 满足(1°)，(3°)得

$$\det_{n-1}C_j=-(\det_{n-1}C)\bar{b}_j\bar{b}_i^{-1}$$

因此

$$(-1)^j(\det_{n-1}C_j)\bar{b}_j^{-1}=(-1)^{j+1}(\det_{n-1}C)\bar{b}_j\bar{b}_i^{-1}\bar{b}_j^{-1}$$
$$=(-1)^i(\det_{n-1}C_i)\bar{b}_j\bar{b}_i^{-1}\bar{b}_j^{-1}$$
$$=(-1)^i(\det_{n-1}C_i)\bar{b}_i^{-1}$$

即 $\det_n$ 与 i 的选取无关，是完全确定的。 □

推论 8.2 除环上的 Dieudonné 行列式存在且惟一，因此满足前述的(1°)，(2°)，(3°)，(4°)，(5°)，(6°)。

命题 8.5　设 $R\in GE_n$ 且满足前述的(1°),(2°),(3°)的 Det 存在,记 $\det_n=\mathrm{Det}|_{GL_n(R)}$,则

(1) $\mathrm{Ker}\det_n=E_n(R)\lhd GL_n(R)$,因此有群同态正合列

$$1\to E_n(R)\to GL_n(R)\xrightarrow{\det_n}R^{\cdot ab}\to 1;\tag{3}$$

(2) $n\geqslant 3$ 时嵌入同态 $R^{\cdot}\to GL_n(R)$ 诱导着一个同构 $R^{\cdot ab}\xrightarrow[\simeq]{}GL_n(R)^{ab}$。

证　(1)由引理 8.2 的(2°)与命题 8.3 的(4°)知 $E_n(R)\subseteq\mathrm{Ker}\det_n$。任取 $A\in\mathrm{Ker}\det_n$,由 $R\in GE_n$ 知 $A=E\mathrm{diag}(d,1,\cdots,1)$,$E\in E_n(R)$,$d\in R^{\cdot}$。于是由(4°),(1°),(3°)知 $\det_n A=\bar{d}$,但 $A\in\mathrm{Ker}\det_n$ 因此 $d\in[R^{\cdot},R^{\cdot}]$。由此知 $\mathrm{diag}(d,1,\cdots,1)\in E_n(R)$(由推论 5.1),故 $A=E\mathrm{diag}(d,1,\cdots,1)\in E_n(R)$,于是 $\mathrm{Ker}\det_n=E_n(R)$。

(2) 由(1)与引理 8.1(3)即得。□

定理 8.1　设 $R\in GE$,且 Dieudonné 行列式存在,则 $K_1(R)\simeq R^{\cdot ab}$。

证　由 Dieudonné 行列式定义中的(c)知,它与 $n\to\infty$ 的极限是相容的,因此由命题 8.5(1)得群同态正合列

$$1\to E(R)\to GL(R)\to R^{\cdot ab}\to 1$$

故 $K_1(R)\simeq R^{\cdot ab}$。□

注②　建议读者由命题 8.5(2)证定理 8.1,并考虑:$R\in SGE$ 时定理 8.1 成立否?

由此定理与命题 8.4 立得

定理 8.2　设 R 为局部环(未必为交换环),则 $K_1(R)\simeq R^{\cdot ab}$。

推论 8.3　设 R 为除环,则 $K_1(R)\simeq R^{\cdot ab}$。

推论 8.4　设 $m=p_1^{n_1}\cdots p_k^{n_k}$,$\mathbb{Z}_m=\mathbb{Z}/m\mathbb{Z}$,$p_1,\cdots,p_k$ 为互异素数.则

$$K_1(\mathbb{Z}_m)\simeq\mathbb{Z}_{p_1^{n_1}}^{\cdot}\oplus\cdots\oplus\mathbb{Z}_{p_k^{n_k}}^{\cdot}(\simeq\mathbb{Z}_m^{\cdot}),$$

其中 $\mathbb{Z}_{p_j^{n_j}}^{\cdot}=\{\bar{a}\,|\,(a,p_j)=1\}$。

证　注意 $\mathbb{Z}_m\simeq\mathbb{Z}_{p_1^{n_1}}\oplus\cdots\oplus\mathbb{Z}_{p_k^{n_k}}$,$\mathbb{Z}_{p_j^{n_j}}$ 为交换局部环即知。□

注③　在§25 中我们将证明:若 $8\nmid m$,则 $\mathbb{Z}_m^{\cdot}$ 为循环群(见引理 25.6),由此可知当 $8\nmid m$ 时 $K_1(\mathbb{Z}_m)$ 为循环群。

§9　Dieudonné 环与半局部环的 K_1 群

上节中我们用 Dieudonné 行列式工具对任意的局部环 R(当然包括除

环),给出了关于 K_1 群的完美结果:$K_1(R)\simeq R^{\cdot ab}$,因此当 R 又为交换环时,$K_1(R)\simeq R^{\cdot}$,对交换的半局部环 R,在 §6 中我们也证明了 $K_1(R)\simeq R^{\cdot}$。但对非交换的半局部环 R,只证出有 $[R^{\cdot},R^{\cdot}]$ 与 $R^{\cdot}$ 的中间群 G 使 $K_1(R)\simeq R^{\cdot}/G$(见定理 6.3)。至于这个 G 如何确定,上几节尚未给出办法。由于半局部环都是 GE 环,用定理 8.1 可知,不能指望用 Dieudonné 行列式解决半局部环的 K_1 群问题,因为对半局部环 $R=\mathbb{Z}_2^{2\times 2}$,Dieudonné 行列式肯定不存在。事实上,$K_1(R)\simeq K_1(\mathbb{Z}_2)=1$ 而 $R^{\cdot ab}\simeq\mathbb{Z}_2$(见后面命题 9.2(3)之证)。若 Dieudonné 行列式存在,则由定理 8.1 知 $K_1(R)\simeq R^{\cdot ab}$,这就得出矛盾。由此也可看出不能将局部环 R 的 $K_1(R)\simeq R^{\cdot ab}$ 向半局部环开拓。因此要想解决半局部环的 K_1 群问题,关键在于另寻它法去定出上述的 G,或者试着找出(非局部环的)特殊的半局部环 R 使 $K_1(R)\simeq R^{\cdot ab}$ 仍成立。我们先从半单 Artin 环入手,由定理 5.4 与定理 5.5 通过 Wedderburn-Artin 定理可立得

命题 9.1 设 S 为半单 Artin 环,则

$$S\simeq R_1^{n_1\times n_1}\oplus\cdots\oplus R_m^{n_m\times n_m},\qquad R_j\text{ 为除环},\ j=1,\cdots,m$$

因此

$$K_1(S)\simeq R_1^{\cdot ab}\oplus\cdots\oplus R_m^{\cdot ab}\simeq(R_1^{\cdot}\oplus\cdots\oplus R_m^{\cdot})^{ab}$$

由上段给出的例子 $\mathbb{Z}_2^{2\times 2}$(单 Artin 环)知,一般地,$(R_1^{\cdot}\oplus\cdots\oplus R_m^{\cdot})^{ab}\neq S^{\cdot ab}$。下面我们希望给出 S 为半单 Artin 环时,使 $K_1(S)\simeq S^{\cdot ab}$ 成立的条件,为此先从命题 8.5(2)出发引入一个定义。

定义 9.1 设 $R\in\mathscr{R}$ing,若嵌入同态 $R^{\cdot}\to GL_n(R)$ 诱导一个群同构

$$R^{\cdot ab}\xrightarrow{\simeq}GL_n(R)^{ab}$$

则称 R 为 **D_n 环**,记为 $R\in D_n$。当对一切 n,R 都是 D_n 环时,则称 R 为 **D 环**(Dieudonné 环),记为 $R\in D$。当对无限多个 n,R 都是 D_n 环时,则称 R 为**稳定 D 环**,记为 $R\in SD$。

由命题 8.5 知当 $n\geqslant 3$,$R\in GE_n$ 且引理 8.2 中的 Det 存在时,$R\in D_n$。由定理 8.1 知,Dieudonné 行列式存在的 SGE 环都是 SD 环。因此,除环,更一般地,局部环(未必为交换环)都是 SD 环。值得注意的是,它们一般地都未必为 D 环。为说明这一点,先通过下述引理来证明除环 $\mathbb{Z}_2\notin D_2$。

引理 9.1 设 G 为任一群,$H\lhd G$,若 G/H 为 Abel 群,则 $H\supseteq[G,G]$,因此有满同态 $G^{ab}\to G/H$ 且按包含关系给出的偏序使

$$[G,G]=\min\{H\mid H\lhd G,G/H\in\mathcal{A}G\},$$

于是 $|G|<\infty$ 时,$|G/H|\mid|G^{ab}|$,$\forall G/H\in\mathcal{A}G$。

证　由 $G/H\in\mathscr{A}G$ 知，$\forall x,y\in G$，在 G/H 中

$$\overline{[x,y]}=[\bar{x},\bar{y}]=\bar{1}$$

因此 $[x,y]\in H$，即 $[G,G]\subseteq H$。 □

命题 9.2　(1) 一切环都是 D_1 环；

(2) 设 R 为除环且 $|R|>2$，则 $R\in D$；

(3) 若 R 为除环且 $|R|=2$（即 $R\simeq\mathbb{Z}_2$ 为二元域），则 $R\in D_n\Leftrightarrow n\neq 2$；

(4) 除环都是 D_n 环，$\forall n\geqslant 3$，因此是 SD 环。

证　(1)是显然的，由(2)，(3)证(4)也是显见的。现在只需证(2)与(3)。

(2) $|R|>2$ 时由 R 为除环知，$\forall 1\neq x\in R$，$x=1+(x-1)\in R^{\cdot}+R^{\cdot}$，又必有 $1\neq a\in R^{\cdot}$，于是 $1=a+(1-a)\in R^{\cdot}+R^{\cdot}$，故 $R=R^{\cdot}+R^{\cdot}$。于是由引理 8.1 知，$\forall n\geqslant 2$，$[GL_n(R),GL_n(R)]=E_n(R)$。由命题 8.5 与推论 8.2 即知 $R\in D_n$，$\forall n\geqslant 2$。再由(1)即知 $R\in D$（注意到除环为 GE_n 环，$\forall n\geqslant 2$）。

(3) 只需证 $R\notin D_2$，可设 $R=\{0,1\}=\mathbb{Z}_2$，于是

$$GL_2(R)=\left\{\begin{pmatrix}1&0\\0&1\end{pmatrix},\begin{pmatrix}1&0\\1&1\end{pmatrix},\begin{pmatrix}1&1\\0&1\end{pmatrix},\begin{pmatrix}1&1\\1&0\end{pmatrix},\begin{pmatrix}0&1\\1&0\end{pmatrix},\begin{pmatrix}0&1\\1&1\end{pmatrix}\right\}$$

$\notin\mathscr{A}G$，为 6 元群，

$$H=\left\{\begin{pmatrix}1&0\\0&1\end{pmatrix},\begin{pmatrix}1&1\\1&0\end{pmatrix},\begin{pmatrix}0&1\\1&1\end{pmatrix}\right\}<GL_2(R),[GL_2(R):H]=2$$

因此 $H\triangleleft GL_2(R)$，$GL_2(R)/H\in\mathscr{A}G$（二元群）。由引理 9.1，Lagrange 定理及 $GL_2(R)\notin\mathscr{A}G$ 知 $[GL_2(R),GL_2(R)]=H$，因此
$|GL_2(R)^{ab}|=2$。但 $R^{\cdot}=1$，因此 $R^{\cdot ab}=1$，于是 $GL_2(R)^{ab}\not\simeq R^{\cdot ab}$，即 $R\notin D_2$。 □

命题 9.3　设有 m 使 $\forall n\geqslant m$，$R\in D_n$，则 $K_1(R)\simeq R^{\cdot ab}$，因此 $R\in D$ 时 $K_1(R)\simeq R^{\cdot ab}$。

证　$\forall n\geqslant m$，有交换图及其 Abel 化（函子 ab 作用）所得的交换图

$$\begin{array}{ccc} & R^{\cdot}=GL_1(R) & \\ \swarrow & & \searrow \\ GL_n(R) & \rightarrowtail & GL_{n+1}(R)\end{array}\quad\overset{ab}{\underset{R\in D_n,\ D_{n+1}}{\Longrightarrow}}\quad\begin{array}{ccc} & R^{\cdot ab} & \\ \swarrow\simeq & & \simeq\searrow \\ GL_n(R)^{ab} & \longrightarrow & GL_{n+1}(R)^{ab}\end{array}$$

由此知 $GL_n(R)^{ab}\simeq GL_{n+1}(R)^{ab}$，$\forall n\geqslant m$，故令 $n\to\infty$ 知

$$K_1(R) = GL(R)^{ab} \simeq R^{*ab}。$$ □

命题 9.4 (1) 设 $R\in D_m\cap D_{mn}$，$S=R^{m\times m}$，则 $S\in D_n$。

(2) 设 $R_j\in D_n$，$j=1,\cdots,k$，则 $R_1\oplus\cdots\oplus R_k\in D_n$。

证 (1) 仿命题 9.3 之证(换那里的 n，$n+1$ 分别为 m，mn)知，嵌入同态 $R^*\to GL_m(R)$，$R^*\to GL_{mn}(R)$诱导出

$$GL_m(R)^{ab} \simeq GL_{mn}(R)^{ab}$$

但 $GL_m(R)^{ab}=S^{*ab}$，$GL_{mn}(R)^{ab}=GL_n(R^{m\times m})^{ab}=GL_n(S)^{ab}$，故 $S\in D_n$。

(2) 只需证 $k=2$ 的情况，只需对交换图

$$\begin{array}{ccc}
R_1^*\oplus R_2^* & \longrightarrow & GL_n(R_1)\oplus GL_n(R_2) \\
\downarrow\simeq & & \downarrow\simeq \\
(R_1\oplus R_2)^* & \longrightarrow & GL_n(R_1\oplus R_2)
\end{array}$$

作 Abel 化，注意 R_1，$R_2\in D_n$，即得

$$\begin{array}{ccc}
R_1^{*ab}\oplus R_2^{*ab} & \xrightarrow{\simeq} & GL_n(R_1)^{ab}\oplus GL_n(R_2)^{ab} \\
\simeq\downarrow & & \downarrow\simeq \\
(R_1^*\oplus R_2^*)^{ab} & & (GL_n(R_1)\oplus GL_n(R_2))^{ab} \\
\simeq\downarrow & & \downarrow\simeq \\
(R_1\oplus R_2)^{*ab} & \xrightarrow{f} & GL_n(R_1\oplus R_2)^{ab}
\end{array}$$

由此知 f 为同构，即 $R_1\oplus R_2\in D_n$。 □

命题 9.5 设 R 为除环，$S=R^{m\times m}$，则

(1) $|R|>2$ 时 $S\in D$；

(2) $|R|=2$ 且 $m\geqslant 3$ 时，$S\in D$；

(3) $|R|=2$ 且 $m=2$ 时 $S\notin D_n$，$\forall n\geqslant 2$。因此 $S\notin SD$，$S\notin D$；

(4) $|R|=2$ 且 $m=1$ 时，$S\in D_n\Leftrightarrow n\neq 2$，因此 $S\in SD\backslash D$；

(5) $S\in D\Leftrightarrow |R|>2$ 或 $|R|=2$ 但 $m\geqslant 3$；

$S\in SD\Leftrightarrow |R|>2$ 或 $|R|=2$ 但 $m\neq 2$；

(6) $m\geqslant 3$ 时 $S\in D$。

证 由命题 9.2 与命题 9.4 即得(1)，(2)，(4)。

(3) 若有 $n\geqslant 2$ 使 $S\in D_n$，则

$$GL_n(S)^{ab} \underset{S\in D_n}{\simeq} S^{*ab} \underset{m=2}{=\!=} GL_2(R)^{ab} \simeq \mathbb{Z}_2 \text{(命题 9.2(3)之证)}$$

但由命题 9.2(3)知

$$GL_n(S)^{ab} \simeq GL_{2n}(R)^{ab} \simeq R^{*ab} = 1。$$

这个矛盾说明(3)肯定成立。

由(1),(2),(3),(4)即得(5)与(6)。 □

由命题 9.3,命题 9.4,命题 9.5 立得关于半单 Artin 环的下述结果。

命题 9.6 设 S 为半单 Artin 环,且 S 无同构于$\mathbb{Z}_2^{2\times 2}$ 的直和项,则

$$K_1(S)\simeq S^{\cdot ab}$$

此时,$S\in D_n$, $\forall n\neq 2$。

值得考虑的一个问题是,对 $R\in \mathrm{Ring}$,会不会出现下述情况:$R\in D_n$,$R\in D_{n+k}$,$k\geqslant 2$,而对 $n<l<n+k$,$R\notin D_l$?

下面来研究半局部环的 K_1 群,由本节第一段与命题 9.3 知 D 环尚不能概括半局部环,还需将 D 环再加推广,找出更大的能概括半局部环的环类。这个新的环类应有助于寻求$[R^{\cdot},R^{\cdot}]$与 $R^{\cdot}$ 的中间群 G,使对半局部环 R 有 $K_1(R)\simeq R^{\cdot}/G$。关键在于(见定理 6.2 前一段)找出特殊的 $R^{\cdot}$ 元素 r,既不限于换位子元素,又能使 $\mathrm{diag}(r,I_{n-1})\in E_n(R)$。为找这种元素需证一条引理。

引理 9.2 设 $R\in \mathrm{Ring}$,$x,y\in R$,则

(1) $\begin{pmatrix}1+xy & \\ & 1\end{pmatrix}\in GL_2(R)\Leftrightarrow\begin{pmatrix}1 & \\ & 1+yx\end{pmatrix}\in GL_2(R)$,即 $1+xy\in R^{\cdot}\Leftrightarrow 1+yx\in R^{\cdot}$;

(2) 设 $1+xy\in R^{\cdot}$,则

$$\begin{bmatrix}1+xy & \\ & (1+yx)^{-1}\end{bmatrix}\in E_2(R),$$

$$\begin{bmatrix}(1+xy)(1+yx)^{-1} & \\ & 1\end{bmatrix}\in E_2(R),$$

因此

$$\begin{bmatrix}(1+xy)(1+yx)^{-1} & \\ & I_{n-1}\end{bmatrix}\in E_n(R)。$$

证 (1)

$$\begin{pmatrix}1+xy & \\ & 1\end{pmatrix}\xrightarrow{\widehat{1}+\widehat{2}\,y}\begin{pmatrix}1+xy & 0\\ y & 1\end{pmatrix}\xrightarrow{\widehat{2}+\widehat{1}\,x}\begin{pmatrix}1+xy & (1+xy)x\\ y & 1+yx\end{pmatrix}$$

$$\xrightarrow{(1)-x(2)}\begin{pmatrix}1 & 0\\ y & 1+yx\end{pmatrix}\xrightarrow{(2)-y(1)}\begin{pmatrix}1 & \\ & 1+yx\end{pmatrix}$$

因此

$$\begin{pmatrix}1 & 0\\ -y & 1\end{pmatrix}\begin{pmatrix}1 & -x\\ 0 & 1\end{pmatrix}\begin{pmatrix}1+xy & \\ & 1\end{pmatrix}\begin{pmatrix}1 & 0\\ y & 1\end{pmatrix}\begin{pmatrix}1 & x\\ 0 & 1\end{pmatrix}=\begin{pmatrix}1 & \\ & 1+yx\end{pmatrix}$$

由此知(1)成立。

(2) 由上式与(命题 6.1(3)之证中的(*))

$$\operatorname{diag}(d_1,d_2,\cdots,d_n)e_{ij}^{x}=e_{ij}^{d_ixd_j^{-1}}\operatorname{diag}(d_1,d_2,\cdots,d_n) \qquad (*)$$

知

$$\begin{pmatrix}1&0\\-y&1\end{pmatrix}\begin{pmatrix}1&-x\\0&1\end{pmatrix}\begin{bmatrix}1&0\\y(1+xy)^{-1}&1\end{bmatrix}$$

$$\begin{pmatrix}1&(1+xy)x\\0&1\end{pmatrix}\begin{pmatrix}1+xy&\\&1\end{pmatrix}=\begin{pmatrix}1&\\&1+yx\end{pmatrix}$$

由此即知

$$\begin{bmatrix}1+xy&\\&(1+yx)^{-1}\end{bmatrix}=\begin{pmatrix}1+xy&\\&1\end{pmatrix}$$

$$\begin{pmatrix}1&\\&1+yx\end{pmatrix}^{-1}\in \mathrm{E}_2(R)$$

但是由推论 5.1(2)知

$$\begin{bmatrix}(1+yx)^{-1}&\\&1+yx\end{bmatrix}\in \mathrm{E}_2(R)$$

于是

$$\begin{bmatrix}(1+xy)(1+yx)^{-1}&\\&1\end{bmatrix}=\begin{bmatrix}1+xy&\\&(1+yx)^{-1}\end{bmatrix}$$

$$\begin{bmatrix}(1+yx)^{-1}&\\&1+yx\end{bmatrix}\in \mathrm{E}_2(R) \qquad \square$$

注① 引理 9.2 中"$1+xy\in R^{\cdot}\Leftrightarrow 1+yx\in R^{\cdot}$"是关键所在,但在思路上难以猜想。分析学家 W. Rudin 认为:想出一个结果后,去证明它,往往并不困难,难的是如何想出这个结果。他专写一文[Rudin,1985]说明如何从特殊情况入手(不必步步思维都顾及严谨性)发现"$1-xy\in R^{\cdot}\Leftrightarrow 1-yx\in R^{\cdot}$"(实质上即"$1+xy\in R^{\cdot}\Leftrightarrow 1+yx\in R^{\cdot}$")。有兴趣的读者读一下该文是有益的。

由推论 5.1 知 $\operatorname{diag}([R^{\cdot},R^{\cdot}],I_{n-1})\subset \mathrm{E}_n(R)$,与引理 9.2(2)相比较,自然要问:$R^{\cdot}$ 中 $(1+xy)(1+yx)^{-1}$ 形的元素生成的乘法子群与 $[R^{\cdot},R^{\cdot}]$ 有何关系? 为方便起见,先给出如下定义(记号):

定义 9.2 设 $R\in$ Ring,记

$$\{(1+xy)(1+yx)^{-1}\mid x,y\in R,\ 1+xy\in R^{\cdot}\}$$

生成的乘法群($R^{\cdot}$ 的子群)为 $v(R)$。

任取 $aba^{-1}b^{-1}\in[R^{\cdot},R^{\cdot}]$，令 $x=a-b^{-1}$，$y=b$，则 $1+xy=ab\in R^{\cdot}$，$1+yx=ba$，于是

$$aba^{-1}b^{-1}=ab(ba)^{-1}=(1+xy)(1+yx)^{-1}\in v(R)$$

故 $[R^{\cdot},R^{\cdot}]\subseteq v(R)$。

又由命题 9.2(3)之证，事实上已知：$R=\mathbb{Z}_2^{2\times 2}$ 时，

$$H=\left\{\begin{pmatrix}1&0\\0&1\end{pmatrix},\begin{pmatrix}1&1\\1&0\end{pmatrix},\begin{pmatrix}0&1\\1&1\end{pmatrix}\right\}=[R^{\cdot},R^{\cdot}]$$

取 $x=\begin{pmatrix}0&0\\0&1\end{pmatrix}$，$y=\begin{pmatrix}1&0\\1&0\end{pmatrix}$，则 $1+xy=\begin{pmatrix}1&0\\1&1\end{pmatrix}$，$1+yx=\begin{pmatrix}1&0\\0&1\end{pmatrix}$。于是

$$(1+xy)(1+yx)^{-1}=\begin{pmatrix}1&0\\1&1\end{pmatrix}\notin H(\text{由此可知 } v(R)=R^{\cdot})。$$

因此，一般地，$[R^{\cdot},R^{\cdot}]\subsetneqq v(R)$。由此可得如下引理：

引理 9.3　设 $R\in$ Ring，则

(1) $[R^{\cdot},R^{\cdot}]\subseteq v(R)\subseteq R^{\cdot}$ 且可能有 $[R^{\cdot},R^{\cdot}]\neq v(R)$；

(2) $v(R)\lhd R^{\cdot}$，因此 $V(R)\equiv R^{\cdot}/v(R)$ 为 Abel 群；

(3) $\mathrm{diag}(v(R),I_{n-1})\subseteq \mathrm{E}_n(R)$。

证　(1) 已由上段证出，(3) 由引理 9.2(2)即得。

(2) 只需证 $av(R)a^{-1}\subseteq v(R)$，$\forall a\in R^{\cdot}$，事实上，$\forall(1+xy)(1+yx)^{-1}\in v(R)$，

$$\begin{aligned}a(1+xy)(1+yx)^{-1}a^{-1}&=a(1+xy)a^{-1}a(1+yx)^{-1}a^{-1}\\&=(1+axya^{-1})(a(1+yx)a^{-1})^{-1}\\&=(1+(axa^{-1})(aya^{-1}))(1+(aya^{-1})(axa^{-1}))^{-1}\in v(R)\end{aligned}$$

再由 $aXYa^{-1}=(aXa^{-1})(aYa^{-1})$，$\forall X,Y\in v(R)$ 及 $v(R)$ 的定义即得(2)。 □

将上述引理用于 D_n 环，可得

命题 9.7　设 $R\in \mathrm{D}_n$，$\forall n\geqslant 3$，则 $v(R)=[R^{\cdot},R^{\cdot}]$，因此

$$V(R)=R^{\cdot ab}$$

证　由交换图(由 $R\in \mathrm{D}_n$ 知其中的 f^{ab} 为同构)

$$\begin{array}{ccc}R^{\cdot} & \xrightarrow{\ f\ } & \mathrm{GL}_n(R)\\ \downarrow & \searrow^{\pi_2 f} & \downarrow{\scriptstyle \pi_2}\\ R^{\cdot ab} & \xrightarrow[f^{ab}]{\cong} & \mathrm{GL}_n(R)^{ab}\end{array}$$

知 $\mathrm{Ker}\,\pi_2 f=[R^{\cdot},R^{\cdot}]\subseteq v(R)$(引理 9.3(1))。而由引理 9.2(2)又知

$$f(v(R)) \underset{(\text{引理}9.2)}{\subseteq} \mathrm{E}_n(R) \underset{(\text{引理}8.1)}{\subseteq}$$
$$[\mathrm{GL}_n(R),\mathrm{GL}_n(R)] \equiv \mathrm{GL}_n(R)' = \mathrm{Ker}\pi_2$$

于是由 f 为单同态知 $v(R) \subseteq \mathrm{Ker}\pi_2 f$，故 $v(R) = \mathrm{Ker}\ \pi_2 f = [R^\cdot, R^\cdot]$。 □

由命题 9.3 与命题 9.7 知：若 $R \in \mathrm{D}$(或有 m 使 $R \in \mathrm{D}_n$，$\forall n \geqslant m$)，则 $\mathrm{K}_1(R) \simeq V(R) = R^{\cdot ab}$，注意 $R = \mathbb{Z}_2^{2\times 2}$ 为半局部环，$\mathrm{K}_1(R) = 1 \not\simeq R^{\cdot ab} \simeq \mathbb{Z}_2$。因此，半局部环 R 未必为 D 环，甚至也未必满足 $R \in \mathrm{D}_n$，$\forall n \geqslant m$。但由上知，对任意环 R，都有 $[R^\cdot, R^\cdot] \lhd v(R) \lhd R^\cdot$。于是，必有满同态 $R^{\cdot ab} \twoheadrightarrow V(R) \equiv R^\cdot / v(R)$，这个 $v(R)$ 事实上即我们前面欲找的中间群 G。上述分析启示我们试着用 $V(R)$ 代替 $R^{\cdot ab}$ 定义一种比 D_n 环更广的环类，使之能概括半局部环。

定义 9.3 设 $R \in \mathrm{Ring}$，嵌入同态 $R^\cdot \to \mathrm{GL}_n(R)$ 诱导出群同构

$$V(R) \equiv R^\cdot / v(R) \xrightarrow{\simeq} \mathrm{GL}_n(R)^{ab},$$

则称 R 为 **D_n' 环**，记为 $R \in \mathrm{D}_n'$。若 $R \in \mathrm{D}_n'$，$\forall n \geqslant 2$，则称 R 为 **D'环**，记为 $R \in \mathrm{D}'$。

由 D_n 环定义与命题 9.7 立得

推论 9.1 $\forall n \geqslant 3$，$\mathrm{D}_n \subset \mathrm{D}_n'$。

现在可以将命题 9.3 推广为

命题 9.8 设有 m 使 $R \in \mathrm{D}_n'$，$\forall n \geqslant m$，则

$$\mathrm{K}_1(R) \simeq V(R) = R^\cdot / v(R)$$

证 由嵌入 $\mathrm{GL}_n(R) \to \mathrm{GL}_{n+1}(R)$ 得群同态 $\mathrm{GL}_n(R)^{ab} \to \mathrm{GL}_{n+1}(R)^{ab}$。又由定义知 $R \in \mathrm{D}_n'$，$\forall n \geqslant m$，$\Leftrightarrow \mathrm{GL}_n(R)^{ab} \simeq V(R)$，$\forall n \geqslant m$。因此

$$\mathrm{K}_1(R) = \mathrm{GL}(R)^{ab} \simeq (\varinjlim \mathrm{GL}_n(R))^{ab}$$
$$\simeq \varinjlim \mathrm{GL}_n(R)^{ab} \simeq \varinjlim V(R) = V(R)$$ □

命题 9.9 设 R 为除环，$S = R^{m\times m}$，则 $S \in \mathrm{D}_n'$，$\forall n \geqslant 3$。

证 由命题 9.5 知：$|R| > 2$ 时 $S \in \mathrm{D} \subset \mathrm{D}_n'$，$\forall n \geqslant 3$；$|R| = 2$，$m \neq 2$ 时 $S \in \mathrm{D}_n \subset D_n'$，$\forall n \geqslant 3$。这里只需考虑 $|R| = m = 2$ 的情况，此时 $|S^\cdot| = 6$(见命题 9.2 之证)，$|[S^\cdot, S^\cdot]| = |H| = 3$ 且 $S^\cdot \supset v(S) \supsetneqq [S^\cdot, S^\cdot]$(见引理 9.3 前一段，那里的 R 是这里的 S)，因此 $v(S) = S^\cdot$，$V(S) = 1$。再注意此时 $R \simeq \mathbb{Z}_2$，$S^\cdot = \mathrm{GL}_2(R) = \mathrm{E}_2(R)$，$\mathrm{GL}_n(S) = \mathrm{GL}_{2n}(R)$，$n \geqslant 3$ 即 $2n \geqslant 6$。由命题 9.2 知 $R \in \mathrm{D}_{2n}$ 即 $\mathrm{GL}_{2n}(R)^{ab} \simeq R^{\cdot ab} = 1$，于是 $\mathrm{GL}_n(S)^{ab} \simeq 1 \simeq V(S)$。即 $S \in \mathrm{D}_n'$，$\forall n \geqslant 3$。 □

命题 9.10 设 $R_j \in \mathrm{D}_n'$，$j = 1, 2, \cdots, m$，则 $R_1 \oplus \cdots \oplus R_m \in \mathrm{D}_n'$。即，$\mathrm{D}_n'$(与 D_n 一样)对 $\oplus$ 也是封闭的。

证 只需证 $m = 2$ 的情况，即设 $R_1, R_2 \in \mathrm{D}_n'$。由 $R_1^\cdot \oplus R_2^\cdot \simeq (R_1 \oplus R_2)^\cdot$

与 $v(R_1)\oplus v(R_2)\simeq v(R_1\oplus R_2)$(群的直积仍以$\oplus$来记)知

$$V(R_1)\oplus V(R_2)\simeq V(R_1\oplus R_2)$$

由 $R_1,R_2\in D_n'$ 知

$$V(R_1)\oplus V(R_2)\simeq GL_n(R_1)^{ab}\oplus GL_n(R_2)^{ab}\simeq GL_n(R_1\oplus R_2)^{ab}$$

因此 $R_1\oplus R_2\in D_n'$。□

由命题 9.9 与命题 9.10 立得

命题 9.11　半单 Artin 环 R 都是 D_n' 环，$\forall n\geqslant 3$。因此，对任意半单 Artin 环 R，$K_1(R)\simeq V(R)$。

注意，由命题 9.5 知$\mathbb{Z}_2^{2\times 2}\notin D_n$，$\forall n\geqslant 2$。再比较命题 9.6，可以看出，$D_n'$ 环比 D_n 环"更能概括"半单 Artin 环。

下面我们将命题 9.11 向半局部环推广，注意对任意半局部环 R，$R/J(R)$为半单 Artin 环，即有限个除环上矩阵环之直积。由命题 9.10 与命题 9.11 知，关键在于：由 $R/J(R)\in D_n'$ 推证 $R\in D_n'$。为此先给出下述结果：

命题 9.12　设 $R\in GE_n$，$n\geqslant 3$，则嵌入同态 $f:R^{\cdot}\longrightarrow GL_n(R)$使下图中的 g 为满同态且 $v(R)\subseteq \mathrm{Ker}g$；同时，$f$ 诱导一个群的满同态$\bar{f}:R^{\cdot}/v(R)=V(R)\twoheadrightarrow GL_n(R)^{ab}$使下图为交换图

$$\begin{array}{ccc}
R^{\cdot} & \xrightarrow{\ f\ } & GL_n(R)\\
{\scriptstyle \pi_1}\downarrow & \searrow{\scriptstyle g=\pi_2 f} & \downarrow{\scriptstyle \pi_2}\\
V(R) & \overset{\bar{f}}{\dashrightarrow} & GL_n(R)^{ab}
\end{array}$$

证　由引理 8.1(或命题 5.1)知，$n\geqslant 3$ 时 $E_n(R)\subseteq GL_n(R)'\equiv[GL_n(R),GL_n(R)]$。而 $R\in GE_n$，由命题 6.2 知 $g=\pi_2 f$ 为满同态，再由引理 9.2(2)又知 $f(v(R))\subseteq E_n(R)\subseteq GL_n(R)'=\mathrm{Ker}\pi_2$ 于是 $g(v(R))=\pi_2 f(v(R))=1$，即 $v(R)\subseteq \mathrm{Ker}g$。因此有满同态$\bar{f}$使上图为交换图。□

由此命题顺便得

推论 9.2　设 $R\in GE_n$，$n\geqslant 3$，则 $R\in D_n'\Leftrightarrow$嵌入同态 $f:R^{\cdot}\to GL_n(R)$诱导的同态$\bar{f}:V(R)\to GL_n(R)^{ab}$为满同态。

命题 9.13　设 $R\in GE_n$，$J=J(R)$，$n\geqslant 3$，$R/J\in D_n'$，则 $R\in D_n'$。

证　由命题 9.12 知，有群同态交换图(其中 g_1，φ_2 为满同态，因此 φ_3 为满同态)

$$\begin{array}{ccccccccc} 1 & \longrightarrow & v(R) & \xrightarrow{i_1} & R^{\cdot} & \xrightarrow{g} & \mathrm{GL}_n(R)^{ab} & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle\varphi_1} & & \downarrow{\scriptstyle\varphi_2} & & \downarrow{\scriptstyle\varphi_3} & & \\ 1 & \longrightarrow & v(R/J) & \longrightarrow & (R/J)^{\cdot} & \xrightarrow{g_1} & \mathrm{GL}_n(R/J)^{ab} & \longrightarrow & 1 \end{array}$$

由 D_n' 环定义知，$R/J\in\mathrm{D}_n'$ 即下行正合，因此只需证上行正合即知 $R\in\mathrm{D}_n'$。为此只需证：$v(R)=\mathrm{Ker}g$。

由命题 9.12 知 $v(R)\subseteq\mathrm{Ker}g$，因此有群同态交换图（其中 φ_2 的限制同态仍记为 φ_2，由 φ_1 满知此 φ_2 满）

$$\begin{array}{ccc} & & \mathrm{Ker}g \\ & \nearrow & \downarrow{\scriptstyle\varphi_2} \\ v(R) & \xrightarrow{\varphi_1} & v(R/J) \end{array}$$

为证 $v(R)=\mathrm{Ker}g$，用反证法。设有 $x\in\mathrm{Ker}g\backslash v(R)$。由 φ_1 满知必有 $y\in v(R)$ 使 $\varphi_2(x)=\varphi_1(y)=\varphi_2(y)$（$\varphi_1$ 可看作是 φ_2 在 $v(R)$ 上的限制），于是可知，$x^{-1}y\in\mathrm{Ker}\varphi_2=1+J$，因此 $x^{-1}y\in\mathrm{Ker}g\cap(1+J)$。若能证明：$\mathrm{Ker}g\cap(1+J)\subseteq v(R)$，则由 $y\in v(R)$ 知 $x^{-1}\in v(R)$，即 $x\in v(R)$，这样就得出矛盾，从而得到 $v(R)=\mathrm{Ker}g$。事实上，任取 $a\in\mathrm{Ker}g\cap(1+J)$，由 $R\in\mathrm{GE}_n$，$n\geqslant 3$ 知 $\mathrm{E}_n(R)=[\mathrm{GL}_n(R),\mathrm{GL}_n(R)]$（见引理 8.1），于是从 $a\in\mathrm{Ker}g$ 知 $\mathrm{diag}(a,1,\cdots,1)\in\mathrm{E}_n(R)\cap(I_n+J^{n\times n})$，再由后面的命题 9.14（其证明不用本命题！）即知 $a\in v(R)$，因此本命题之证可告结束。 □

为介绍命题 9.14，先介绍两个记号，这是相对 K_1 群及同余子群理论中的基本记号。

定义 9.4 设 $R\in\mathrm{Ring}$，$J\lhd R$，$\pi:R\to R/J$ 为标准同态，$f=\mathrm{GL}_n(\pi)$：$\mathrm{GL}_n(R)\to\mathrm{GL}_n(R/J)$ 为 π 诱导的群同态。记

$$\mathrm{GL}_n(R,J)=\mathrm{Ker}f(=I_n+J^{n\times n})$$

称为 $\mathrm{GL}_n(R)$ 的由 J 确定的（J 上的，J 水平的）**主同余子群**（principal congruence subgroup）

$$\begin{aligned}\mathrm{E}_n(R,J)&=\mathrm{E}_n(R)\cap\mathrm{GL}_n(R,J)\\&=\langle\{e_{il}^a\mid\forall a\in J,i\neq l,1\leqslant i,l\leqslant n\}\rangle\\&=\mathrm{E}_n(R)\cap(I_n+J^{n\times n})\end{aligned}$$

$E_n(R,J)$与 $GL_n(R,J)$之间的 $GL_n(R)$之子群 H 称为是水平为 J 的子群。当 $n\geqslant 2$ 时 H 的水平是惟一确定的，即 $E_n(R,J)\subset GL_n(R,J')$时必有 $J\subset J'$，著名的三明治定理(sandwich theorem)即：$E_n(R)$正规化 $GL_n(R)$的子群 $H\Leftrightarrow E_n(R,A)\subset H\subset GL_n(R,A)'$（$GL_n(R,A)$的换位子群）对惟一的 $A\lhd R$ 成立。1982 年 A. Bak 将此推广为：在 R 的一个稳定度条件下，H 由 $E_n(R,B)$正规化$\Leftrightarrow E_n(R,AB^{24})\subset H\subset GL_n(R,A)'$，$\forall A\lhd R,B\lhd R$。1987 年李福安与刘木兰在[Li,1987]进一步证明了：H 由 $E_n(R,B)$正规化$\Leftrightarrow$对充分大的 m，$E_n(R,AB^m)\subset H\subset GL(R,A)'$（$GL(R,A)$的换位子群）。

注①　$K_1(R,J)\equiv GL_n(R,J)/E_n(R,J)$称为 R 对 J 的**相对 K_1 群**，$\forall J\lhd R$。

命题 9.14　设 $R\in$ Ring，$J=J(R)$（或更一般地，设 $J\lhd R$ 使 $1+J\subseteq R^{\cdot}$，即 $J\subseteq J(R)$）。则有群同态

$$\det: GL_n(R,J)\to V(R)\equiv R^{\cdot}/v(R),\qquad \forall n\geqslant 1$$

满足

(a) $E_n(R,J)\subset \operatorname{Ker}\det$；

(b) $\det\operatorname{diag}(a_1,\cdots,a_n)=\overline{a_1\cdots a_n}$，$\forall a_j\in 1+J$，$\bar{x}$ 表同余类 $x \bmod v(R)$，$\forall x\in R$；

(c) 有交换图

$$\begin{array}{ccc} GL_n(R,J) & \xrightarrow{i} & GL_{n+1}(R,J) \\ & \det\searrow \quad \swarrow\det & \\ & V(R) & \end{array}$$

其中 i 表标准嵌入（使 $i(A)=\begin{pmatrix} A & \\ & 1\end{pmatrix}$，$\forall A\in GL_n(R,J)$）；

(d) $\forall \alpha\in J^{n\times 1}$，$\beta\in J^{1\times n}$，$\det(I_n+\alpha\beta)=\overline{1+\beta\alpha}$。

证　用归纳法具体构作 det。

$m=1$ 时 $GL_1(R,J)=1+J$。定义

$$\det: 1+J\to V(R)$$
$$1+j\mapsto 1+j\ (\bmod v(R))$$

则容易看出 det 为群同态且满足(a)，(b)，(d)。下面对包括 $m=2$ 的情况定义出 det 后易见(c)也成立。

下设 $m\leqslant n$ 时已构作出 det 满足(a)，(b)，(c)，(d)（$m=n$ 时暂不考虑(c)）。来作 $m=n+1$ 时的 det 使(a)，(b)，(d)以及 $m=n$ 时的(c)成立。注意 $M=(m_{ij})\in GL_{n+1}(R,J)$，则 $M\equiv I_{n+1}(\bmod J)$。于是可将 M 写成惟一

确定的下形，进行分解。

$$M=\begin{pmatrix} A+\alpha\beta & \alpha \\ a\beta & a \end{pmatrix}\xrightarrow[\hat{1}\ -\ \hat{2}\ \beta]{\text{块初等列变换}}\begin{pmatrix} A & \alpha \\ & a \end{pmatrix}\Rightarrow M=\begin{pmatrix} A & \alpha \\ & a \end{pmatrix}\begin{pmatrix} I_n & \\ \beta & 1 \end{pmatrix}$$

其中 $a=m_{n+1,n+1}\equiv 1(\bmod J)$，于是 a^{-1} 存在，$\alpha=(m_{1,n+1},m_{2,n+1},\cdots,m_{n,n+1})^T\in J^{n\times 1}$，$\beta=a^{-1}(m_{n+1,1},m_{n+1,2},\cdots,m_{n+1,n})\in J^{1\times n}$，$A+\alpha\beta$ 为 M 去掉末行、末列得到的 $n\times n$ 主子矩阵。定义映射

$$\det:\mathrm{GL}_{n+1}(R,J)\to V(R)$$
$$M\mapsto \bar{a}\det A$$

显然，这是完全确定的映射且当 $m=n$ 时(c)必成立。下证它为群同态，再任取 $N\in\mathrm{GL}_{n+1}(R,J)$ 且仿上将 N 写成惟一确定的下形

$$N=\begin{pmatrix} B+\alpha_1\beta_1 & \alpha_1 \\ b\beta_1 & b \end{pmatrix},\ \alpha_1\in J^{n\times 1},\ \beta_1\in J^{1\times n}$$

则 $MN=\begin{pmatrix} (AB-A\alpha_1(\beta\alpha_1+b)^{-1}\beta B)+\alpha_2\beta_2 & \alpha_2 \\ a(\beta\alpha_1+b)((\beta\alpha_1+b)^{-1}\beta B+\beta_1) & a(\beta\alpha_1+b) \end{pmatrix}$，其中 $\beta_2=(\beta\alpha_1+b)^{-1}\beta B+\beta_1$。注意 $\bar{a},\bar{b},\overline{ab},\det A,\det B$ 都是 Abel 群 $V(R)$ 中元素，可以看出，$AB-A\alpha_1(\beta\alpha_1+b)^{-1}\beta B=A(I_n-\alpha_1(\beta\alpha_1+b)^{-1}\beta)B$ 在 det 下的象($m=n$ 情况)为 $\det A\cdot\det B\cdot\overline{(1-(\beta\alpha_1+b)^{-1}\beta\alpha_1)}$，于是由上述定义知

$$\begin{aligned}\det(MN)&=\bar{a}\det A\cdot\overline{(\beta\alpha_1+b)}\cdot\overline{(1-(\beta\alpha_1+b)^{-1}\beta\alpha_1)}\det B\\&=(\bar{a}\det A)(\bar{b}\det B)=\det M\cdot\det N\end{aligned}$$

即 det 对 $m=n+1$ 也是群同态且显然满足(a),(b),(c)。下面证明 $m=n+1$ 时(d)也成立，即 $\forall\alpha\in J^{(n+1)\times 1}$，$\beta\in J^{1\times(n+1)}$ 来证 $\det(I_{n+1}+\alpha\beta)=\overline{1+\beta\alpha}$。为此记 $\alpha=(\alpha_1,a)^T$，$\beta=(\beta_1,b)$，则 $\alpha_1\in J^{n\times 1}$，$\beta_1\in J^{1\times n}$，$a,b\in J$。显然有 $I_{n+1}+\alpha\beta\in\mathrm{GL}_{n+1}(R,J)$ 且

$$\begin{aligned}I_{n+1}+\alpha\beta&=I_{n+1}+\begin{pmatrix}\alpha_1\beta_1 & \alpha_1 b\\ a\beta_1 & ab\end{pmatrix}\\&=\begin{pmatrix}I_n+\alpha_1\beta_1 & \alpha_1 b\\ a\beta_1 & 1+ab\end{pmatrix}=\begin{pmatrix}A+\alpha_3\beta_3 & \alpha_3\\ (1+ab)\beta_3 & 1+ab\end{pmatrix}\end{aligned}$$

其中

$$\begin{aligned}\alpha_3&=\alpha_1 b,\beta_3=(1+ab)^{-1}a\beta_1\\A&=I_n+\alpha_1\beta_1-\alpha_1 b(1+ab)^{-1}a\beta_1\\&=I_n+\alpha_1(1-b(1+ab)^{-1}a)\beta_1\end{aligned}$$

而由易于验证(展开并提因子)的恒等式

$$(1+yx)(1-y(1+xy)^{-1}x)$$
$$=(1-y(1+xy)^{-1}x)(1+yx)=1$$

知 $1-b(1+ab)^{-1}a=(1+ba)^{-1}$。于是(对 $m=n$ 的情况)

$$\det A=\overline{1+(1+ba)^{-1}\beta_1\alpha_1}$$

又按 det 对 $m=n+1$ 情况的定义,并注意 $(1+ab)(1+ba)^{-1}\in v(R)$,即 $\overline{(1+ab)(1+ba)^{-1}}=\overline{1}$,即得

$$\det(I_{n+1}+\alpha\beta)=\overline{1+ab}\det A=\overline{1+ab}\ \overline{1+(1+ba)^{-1}\beta_1\alpha_1}$$
$$=\overline{(1+ab)(1+ba)^{-1}}\ \overline{(1+ba)+\beta_1\alpha_1}$$
$$=\overline{1+\beta_1\alpha_1+ba}=\overline{1+\beta\alpha}$$

于是命题证毕。 □

由命题 9.11,命题 9.13 与命题 9.8 立得下述结果(见[Silvester, 1981])。

定理 9.1　半局部环 R(未必为交换环)都是 D_n' 环,$\forall n\geqslant 3$,因此

$$K_1(R)\simeq V(R)\equiv R^{\cdot}/v(R)$$

1984 年 P. Menal 与 J. Moncasi 在[Menal, 1984]中引进幺稳定度为 1 的环类 uSr1,即若 $a,b\in R$,有 $x\in R$ 使 $ax+b=1$,则必有 $u\in R^{\cdot}$ 使 $a+bu\in R^{\cdot}$,此时称 R 的幺稳定度为 1,记为 $R\in u\mathrm{Sr}1$,或 $u\mathrm{Sr}(R)=1$。他们证明了:此时必有 $K_1(R)\simeq V(R)$。显然 $u\mathrm{Sr}1\subseteq \mathrm{Sr}1$ 但反之不成立(比如取 $R=\mathbb{Z}_2$)。1994 年武同锁在[武同锁, 1994]证明了:设 R 为半局部环,则 $R\in u\mathrm{Sr}1\Leftrightarrow\mathbb{Z}_2$ 不是 R 的同态象。由上可看出,定理 9.1 的结果是相当好的,对半局部环,至今仍未见有优于这个结果的工作。

此外,若有 m 使 $R\in D_n'$,$\forall n\geqslant m$,可证明有满足 Dieudonné 行列式(定义 8.1)的特征性质(a),(b),(c)(将$[R^{\cdot},R^{\cdot}]$改为 $v(R)$)的行列式同态 $\det:GL_n(R)\to V(R)$,$\forall n\geqslant m$。最后,我们提出一个值得研究的问题,能否证出或推翻:设 R 为半局部环,则 $K_1(R)\simeq R^{\cdot ab}\Leftrightarrow R$ 无同构于$\mathbb{Z}_2^{2\times 2}$ 的同态象?陈卫星已用两个反例给以彻底的推翻(见他 2004 年在南京大学的博士论文)。

第三章　K_2 群的基础理论与 K_i 群的同调刻画

在上一章中我们已看到初等群 E(R)对 $K_1(R)$所起的重要作用。本章仍从 E(R)出发，取出其元素一定满足的常用的三种关系，形式上地定义 Steinberg 群 St(R)(对应于 E(R)的生成元 e_{ij}^a，用 $x_{ij}(a)$作为 St(R)的生成元)。于是有标准同态 ϕ:St(R) $\twoheadrightarrow$ E(R)使 $\phi(x_{ij}(a))=e_{ij}^a$。Kerϕ 就是我们定义的 $K_2(R)$。事实上，它就是 St(R)的中心 C(St(R))(见 § 10)，也是 E(R)的泛中心扩张的核(见 § 11)。作为环范畴到 Abel 群范畴的函子，K_2 也有上章开头提到的 K_0，K_1 的那些共性。在 § 12 中我们还给出了 K_2 群以及 K_1 群的同调刻画。为此，从同调角度又可将 K_1，K_2 函子看成是同调函子，从中又可看出同调理论与代数 K 理论的紧密联系。在 § 13 中我们还证明了 K_i 群($i=0,1,2$)关于正向极限的连续性。由于直和、推出(图)都是特殊的正向极限，这些结果的概括性与应用广泛性是可想而知的。此外，在 § 14，以 K_0 群为例，我们介绍了代数 K 理论与拓扑 K 理论的紧密联系，从中也可体味出从范畴高度研究问题的重要性。在下一章我们即从范畴的高度来介绍 K_i 群($i=0,1$)及它们之间有重要应用的正合列。

§ 10　Steinberg 群与 K_2 群

在前面五节中我们已看到：对环 R，$E_n(R)$在定义与计算 K_1 群方面有重要地位。现在我们再从另一角度看 $E_n(R)$。作为群，$E_n(R)$有生成系(生成元集)$\{e_{ij}^a \mid a\in R, i\neq j, 1\leqslant i,j\leqslant n\}$，这些生成元(即初等矩阵)间有着丰富的关系，比如 $e_{ij}(a)e_{ij}(b)=e_{ij}(a+b)$等(见引理 5.2)。任一群 G 都可由其

生成系及生成元之间的关系集(也称为 G 的关系集)来刻画,记 S 为 $E_n(R)$ 的关系集,R 的性质在相当程度上决定着 $E_n(R)$ 与 S。比如 R 为域时,$\forall A \in SL_n(R)$(即 $\det A=1$)都可表为 $E_n(R)$ 的生成元之积(即 $SL_n(R)=E_n(R)$),但对一般的交换环这是办不到的。为此,我们从 S 中取出一部分(对一切环 R 都有的)关系(即这一关系的集合 S' 为 S 的子集),令 $\{x_{ij}(a)\}$ 与 $\{e_{ij}^a\}$ 为 1－1 对应的集,以 $\{x_{ij}(a)\}$ 作生成系,以 S' 为关系集则得到一个新的群(下面记为 $St_n(R)$),当然由 $x_{ij}^{(a)}\mapsto e_{ij}^a$ 给出 $St_n(R)$ 到 $E_n(R)$ 的一个标准同态,其核即度量着 $St_n(R)$ 与 $E_n(R)$ 的关系集的差距,对 $E_n(R)$ 通过 §5 中的取极限(取无穷并)的办法,即可给出环 R 的另一个不变量 $K_2(R)$。更具体地说,取引理 5.2 中的三个关系(2),(3),(4)作 S',先给出如下定义,其中(S_1)主要用于合成,(S_2)主要用于交换,而(S_3)主要用于交换与相似变换(内自同构)。

定义 10.1 设 $R\in$ Ring,$St(R)$ 为由 $\{x_{ij}(a)\mid i\neq j, a\in R\}$ 作生成系且按下述关系定义的乘法群:

(S_1) $x_{ij}(a)x_{ij}(b)=x_{ij}(a+b)$, $\forall a,b\in R$;

(S_2) $[x_{ij}(a),x_{kl}(b)]=1$, $\forall a,b\in R, i\neq l, j\neq k$;

(S_3) $[x_{ij}(a),x_{jl}(b)]=x_{il}(ab)$, $\forall a,b\in R, i\neq l$。

则称 $St(R)$ 为 R 的 **Steinberg 群**,且称(S_1),(S_2),(S_3)为 **Steinberg 关系**。

命题 10.1 设 $R\in$ Ring,则 $St(R)$ 为完全群,即 $[St(R),St(R)]=St(R)$。

证 在(S_3)中取 $b=1$ 得

$$x_{il}(a)=[x_{ij}(a),x_{jl}(1)]\in[St(R),St(R)]$$

由此知 $St(R)\subseteq[St(R),St(R)]\subseteq St(R)$,因此 $St(R)$ 为完全群。 □

定义 10.2 [Milnor] 设 $R\in$ Ring,对标准满同态

$$\phi: St(R)\to E(R)$$

$$x_{ij}(a)\mapsto e_{ij}^a$$

记 $K_2(R)=\mathrm{Ker}\phi$,称 $K_2(R)$ 为 R 的 **K_2 群**,常称 ϕ 为 **Steinberg 同态**。

若限制 $1\leqslant i,j\leqslant n$,则记 $St_n(R)$ 为由 $\{x_{ij}(a)\mid a\in R, i\neq j, 1\leqslant i,j\leqslant n\}$ 以(S_1),(S_2),(S_3)作关系集生成的群,$\phi_n=\phi|_{St_n(R)}$,$K_{2,n}(R)=\mathrm{Ker}\phi_n$。

注① 1989 年李福安在[Li,1989]中证明了:对交换环 R 与 S,(1) 若 $St_m(R)\simeq St_n(S)$,则 $m=n$;(2) $St_n(R)\simeq St_n(S)$, $\forall n\geqslant 4 \Leftrightarrow R\simeq S$,此时必有 $K_{2,n}(R)\simeq K_{2,n}(S)$。他还在[Li,1992]中给出 $E_n(R)$ 与 $St_n(R)$ 的一些有趣的子群分解式。1992 年游宏在[You,1992]中又以 $E_n(R)$,$St_n(R)$ 的分解式出色地刻画了局部环 R。

比较 $K_1(R)$与 $K_2(R)$的定义，视 ϕ 为 $\phi_1: \mathrm{St}(R)\to \mathrm{GL}(R)$即得

定理 10.1 设 $R\in \mathfrak{R}\mathrm{ing}$，则有群同态正合列

$$1 \to K_2(R) \to \mathrm{St}(R) \xrightarrow{\phi} E(R) \to 1$$

$$1 \to K_2(R) \to \mathrm{St}(R) \xrightarrow{\phi_1} \mathrm{GL}(R) \to K_1(R) \to 1$$

$$x_{ij}(a) \longmapsto e_{ij}^{a}$$

由此知，ϕ_1（事实上即 ϕ，但值域不同）犹如一根扁担同时挑起 $K_2(R)$与 $K_1(R)$，$K_2(R)$是 $\mathrm{St}(R)$的关系集与 $E(R)$的关系集相差程度的度量，为 ϕ_1（或 ϕ）的核 $\ker\phi_1$，而 $K_1(R)=\mathrm{Coker}\phi_1=\mathrm{GL}(R)/\mathrm{Im}\phi_1$ 为 ϕ_1 的上核，度量着 ϕ_1 满的程度。

下一命题又说明 $K_2(R)$为 $\mathrm{St}(R)$交换程度（中心大小）的度量。

命题 10.2 设 $R\in \mathfrak{R}\mathrm{ing}$，$C(G)$表示群 G 的中心，则

(1) $C(E(R))=1$（即 $E(R)$为交换程度最差的群）；

(2) $C(\mathrm{St}(R))=K_2(R)$，因此 $K_2(R)$为 Abel 群。

证 (1) 令 $N\in C(E(R))$，则有充分大的 n 使（可视为）$N\in E_n(R)$，

$$\begin{pmatrix} N & \\ & I_n \end{pmatrix}\in E_{2n}(R) \quad 且 \quad \begin{pmatrix} N & \\ & I_n \end{pmatrix}\in C(E_{2n}(R))$$

取 $\begin{bmatrix} I_n & I_n \\ & I_n \end{bmatrix}\in E_{2n}(R)$，则

$$\begin{pmatrix} N & N \\ & I_n \end{pmatrix}=\begin{pmatrix} N & \\ & I_n \end{pmatrix}\begin{bmatrix} I_n & I_n \\ & I_n \end{bmatrix}=\begin{bmatrix} I_n & I_n \\ & I_n \end{bmatrix}\begin{pmatrix} N & \\ & I_n \end{pmatrix}=\begin{bmatrix} N & I_n \\ & I_n \end{bmatrix}$$

于是 $N=I_n$，因此 $C(E(R))=1$。

(2) 令 $M\in C(\mathrm{St}(R))$，$\phi(M)=N\in E(R)$。由 ϕ 满知 $N\in C(E(R))=1$，于是 $M\in \mathrm{Ker}\phi=K_2(R)$，因此 $C(\mathrm{St}(R))\subseteq K_2(R)$。

下证反包含关系。

(i) 记$\mathfrak{C}_n$ 为由$\{x_{in}(a)\mid i\neq n, a\in R\}$生成的 $\mathrm{St}(R)$之子群。

由(S_2)知$[x_{in}(a), x_{in}(b)]=[x_{in}(a), x_{jn}(c)]=1$，$\forall a,b,c\in R$，因此$\mathfrak{C}_n\in \mathfrak{Ab}G$。

(ii) $\forall Y, Y_1\in \mathfrak{C}_n$，$Y\neq Y_1$，则可令 $Y=\prod\limits_{i\neq n} x_{in}(a_i)$，若 Y 的分解式中不含足码对(j,n)，则取 $a_j=0$。（由(S_1)知 $x_{jn}(0)x_{jn}(0)=x_{jn}(0)$，于是 $x_{jn}(0)=1$），$Y_1=\prod\limits_{i\neq n} x_{in}(b_i)$，于是 $\phi(Y_1)=\prod\limits_{i\neq n} e_{in}^{a_i}$ 的第 n 列为 $A=(a_1,\cdots,a_{n-1},1,a_{n+1},\cdots)^T$，$\phi(Y_1)=\prod\limits_{i\neq n} e_{in}^{b_i}$ 的第n 列为$B=(b_1,\cdots,b_{n-1},1,b_{n+1},\cdots)^T$。由 $Y\neq$

Y_1 知 $A \neq B$,即 $\phi(Y) \neq \phi(Y_1)$,因此 $\phi|_{\mathscr{C}_n}$ 是单的。

(iii) $\forall\, p \neq n, p \neq q$ 由

$$x_{pq}(a)x_{in}(b)x_{pq}(a)^{-1} = [x_{pq}(a), x_{qn}(b)]x_{in}(b)$$
$$= \begin{cases} x_{in}(b) \in \mathscr{C}_n, & \forall\, q \neq i \\ x_{pn}(ab)x_{in}(b) \in \mathscr{C}_n, & q = i \end{cases}$$

知,$x_{pq}(a)$正规化 $\mathscr{C}_n$。

任取 $\alpha \in K_2(R)$,即 $\phi(\alpha) = I$。由 α 为 $St(R)$的(有限个)生成元之积知,必有充分大的 n 使 n 大于 α 的表示式中出现的一切生成元 $x_{ij}(a)$的足码 i, j。由上知 α 正规化 $\mathscr{C}_n$,即 $\alpha\mathscr{C}_n\alpha^{-1} \subset \mathscr{C}_n$,又 $\forall\, \beta \in \mathscr{C}_n$,

$$\phi(\alpha\beta\alpha^{-1}) \xlongequal[\phi(\alpha)=I]{} \phi(\beta)$$

由(ii)证出的 $\phi|_{\mathscr{C}_n}$ 单性知 $\alpha\beta\alpha^{-1} = \beta$,即 $\alpha\beta = \beta\alpha$, $\forall\, \beta \in \mathscr{C}_n$,于是 $\alpha \in C(\mathscr{C}_n)$。

(iv) 类似地,记 $\mathscr{R}_n$ 为由$\{x_{nj}(a) \mid j \neq n, a \in R\}$生成的 $St(R)$之子群,则 $\forall\, \alpha \in K_2(R)$必有充分大的 n 使 $\alpha \in C(\mathscr{R}_n)$。

(v) 为证 $K_2(R) \subset C(St(R))$只需再证 $\mathscr{C}_n$, $\mathscr{R}_n$ 生成 $St(R)$。

事实上 $\forall\, p \neq q$, $p = n$ 时 $x_{pq}(a) \in \mathscr{R}_n$, $q = n$ 时 $x_{pq}(a) \in \mathscr{C}_n$,而 $p, q \neq n$ 时,$x_{pq}(a) = [x_{pn}(a), x_{nq}(1)] \in [\mathscr{C}_n, \mathscr{R}_n]$,于是 $\mathscr{C}_n$, $\mathscr{R}_n$ 生成 $St(R)$。 □

注②　注意 G 为完全群 $\not\Rightarrow C(G) = 1$。比如 F 为域 $|F| > 3$, $SL_2(F)$为完全群,但 $C(SL_2(F))$为 2 阶群。

命题 10.2 使我们已走到中心扩张的大门口,现在给其定义如下。

定义 10.3　设 $\varphi: E \to G$ 为群的满同态,若 $\text{Ker}\varphi \subseteq C(E)$(因此 $\text{Ker}\varphi$ 为 Abel 群),则称(E, φ)(或 E 或 φ)为 G 的**中心扩张**(central extension),记为$(E, \varphi) \in c.e(G)$。

若(E, φ)又满足泛性质(即(E, φ)为 G 的全体中心扩张所成范畴的始对象):任给$(E_1, \theta) \in c.e(G)$必有惟一的群同态 $\psi: E \to E_1$ 使下图为交换图,

$$\begin{array}{ccc} E & \xrightarrow{\varphi} & G \\ & {\scriptstyle \exists 1\psi} \searrow \quad \nearrow {\scriptstyle \forall\theta} & \\ & E_1 & \end{array}$$

则称(E, φ)(或 E,或 φ)为 G 的**泛中心扩张**(universal central extension),记为$(E, \varphi) \in u.c.e(G)$。

显然,G 若有泛中心扩张,则在同构意义下,泛中心扩张是惟一的。

注③　在定义 10.3 条件下,有的文献上也称 G 为 E 的中心扩张。用正合列 $1 \to K \to E \to G \to 1$ 定义的扩张也有两种说法,一称这是 K 按 G(of K

by G)的扩张(如[Rotman,1979],[佟文廷,1998]),这与实际情况(E>K)相符)。一称这是 G 按 K(of G by K)的扩张(如[Rosenberg,1994]),这与群的上同调记号一致。两说法各有优缺点,读者在阅读各文献时应注意鉴别。

由上述定义可将命题 10.2 写成如下的(较弱)形式。

命题 10.2′ $(\mathrm{St}(R),\phi)$为 $\mathrm{E}(R)$的中心扩张,即

$$(\mathrm{St}(R),\phi)\in \mathrm{c.e}(\mathrm{E}(R))。$$

下节中将证明$(\mathrm{St}(R),\phi)\in \mathrm{u.c.e}(\mathrm{E}(R))$。

现在来讨论 K_2 的函子性质。

定理 10.2 (1) $\mathrm{St}:\mathrm{Ring}\to \mathrm{G}$ 为共变函子;

(2) $\mathrm{K}_2:\mathrm{Ring}\to \mathrm{AbG}$ 为共变函子。

证 容易直接验证 $\mathrm{St}:\mathrm{Ring}\to \mathrm{G}$ 为共变函子。在此基础上,设有环同态 $f:R\to S$ 与 $g:S\to T$,则有群同态交换图

$$\begin{array}{ccccccccc}
1 & \longrightarrow & K_2(R) & \xrightarrow{i_1} & St(R) & \xrightarrow{\phi_R} & E(R) & \longrightarrow & 1\\
 & & \downarrow{\scriptstyle K_2(f)} & & \downarrow{\scriptstyle St(f)} & & \downarrow{\scriptstyle E(f)} & & \\
1 & \longrightarrow & K_2(S) & \xrightarrow{i_2} & St(S) & \xrightarrow{\phi_S} & E(S) & \longrightarrow & 1\\
 & & \downarrow{\scriptstyle K_2(g)} & & \downarrow{\scriptstyle St(g)} & & \downarrow{\scriptstyle E(g)} & & \\
1 & \longrightarrow & K_2(T) & \xrightarrow{i_3} & St(T) & \xrightarrow{\phi_T} & E(T) & \longrightarrow & 1
\end{array}$$

用图追踪(方法与模论中的图追踪相同)建立 $\mathrm{K}_2(f)$,$\mathrm{K}_2(g)$使上图仍为交换图,即知 $\mathrm{K}_2(gf)=\mathrm{K}_2(g)\mathrm{K}_2(f)$。以建立 $\mathrm{K}_2(f)$为例:$\forall x\in \mathrm{K}_2(R)$,当然 $i_1(x)\in \mathrm{St}(R)$,于是 $y\equiv \mathrm{St}(f)(i_1(x))\in \mathrm{St}(S)$。下证 $y\in \mathrm{Ker}\phi_S=\mathrm{K}_2(S)$ 后,定义 $\mathrm{K}_2(f)(x)=y$ 即可。事实上,由 $\phi_R(i(x))=1$ 知 $\mathrm{E}(f)\phi_R(i(x))=1$。由上图右上角方框图的交换性即知 $\phi_S(y)=1$ 即 $y\in \mathrm{Ker}\phi_S=\mathrm{K}_2(S)$。

又显见 $\mathrm{K}_2(I_R)=I_{\mathrm{K}_2(R)}$,故 $\mathrm{K}_2:\mathrm{Ring}\to \mathrm{AbG}$(由命题 10.2,$\mathrm{K}_2(R)\in \mathrm{AbG}$)为共变函子。 □

定理 10.3 设 $R,S,R_j\in \mathrm{Ring}$,则

(1) $\mathrm{St}(R\oplus S)\simeq \mathrm{St}(R)\oplus \mathrm{St}(S)$,因此 $\mathrm{St}(\bigoplus_{j=1}^{n}R_j)\simeq \bigoplus_{j=1}^{n}\mathrm{St}(R_j)$;

(2) $\mathrm{K}_2(R\oplus S)\simeq \mathrm{K}_2(R)\oplus \mathrm{K}_2(S)$,因此 $\mathrm{K}_2(\bigoplus_{j=1}^{n}R_j)\simeq \bigoplus_{j=1}^{n}\mathrm{K}_2(R_j)$。

证 (1) 显然有群的单同态

$$\mathrm{St}(R)\to \mathrm{St}(R\oplus S),\qquad \mathrm{St}(S)\to \mathrm{St}(R\oplus S)$$

$$x_{ij}(r)\mapsto x_{ij}(r,0)\qquad\qquad x_{ij}(s)\mapsto x_{ij}(0,s)$$

于是可令

$$\mathrm{St}(R)=\langle\{x_{ij}(r,0)\mid r\in R,\ i\neq j\}\rangle<\mathrm{St}(R\oplus S)$$

$$\mathrm{St}(S)=\langle\{x_{ij}(0,s)\mid s\in S,\ i\neq j\}<\mathrm{St}(R\oplus S)$$

由

$$x_{ij}(r,s)=x_{ij}(r,0)x_{ij}(0,s)$$

知

$$\mathrm{St}(R\oplus S)=\langle\mathrm{St}(R),\mathrm{St}(S)\rangle$$

为证 $\mathrm{St}(R\oplus S)\simeq\mathrm{St}(R)\oplus\mathrm{St}(S)$，只需再证 $\mathrm{St}(R)\lhd\mathrm{St}(R\oplus S)$，$\mathrm{St}(S)\lhd\mathrm{St}(R\oplus S)$ 且 $\mathrm{St}(R)\cap\mathrm{St}(S)=1$。

先证 $\mathrm{St}(R)\lhd\mathrm{St}(R\oplus S)$，$\mathrm{St}(S)\lhd\mathrm{St}(R\oplus S)$。为此只需证明在 $\mathrm{St}(R\oplus S)$ 中 $\mathrm{St}(R)$ 中元素与 $\mathrm{St}(S)$ 中元素对乘法可交换，即 $\forall r\in R,s\in S,i\neq j,k\neq l$，

$$y=[x_{ij}(r,0),x_{kl}(0,s)]=1。$$

(i) 当 $i\neq l,j\neq k$ 时，由 (S_2) 知此式成立。

(ii) 当 $i\neq l$ 但 $j=k$ 时，由 (S_3) 知

$$y=x_{il}((r,0)(0,s))=x_{il}(0,0)$$

但 $x_{il}(0,0)x_{il}(0,0)\underset{(S_1)}{=\!=}x_{il}(0,0)$。消去 $x_{il}(0,0)$ 即知 $x_{il}(0,0)=1$，于是此时欲证之式也成立。

(iii) 当 $i=l$ 但 $j\neq k$ 时，

$$\begin{aligned}y&=[x_{ij}(r,0),x_{ki}(0,s)]\\&=[x_{ki}(0,s),x_{ij}(r,0)]^{-1}\underset{(\text{由上})}{=\!=\!=}1^{-1}=1\end{aligned}$$

(iv) 当 $i=l$ 且 $j=k$ 时

$$\begin{aligned}y&=[x_{ij}(r,0),x_{ji}(0,s)]\underset{(S_2)}{=\!=}[x_{ij}(r,0),[x_{jm}(0,s),x_{mi}(0,1)]],m\neq i,j\\&=x_{ij}(r,0)x_{jm}(0,s)x_{mi}(0,1)x_{jm}(0,s)^{-1}x_{mi}(0,1)^{-1}x_{ij}(r,0)^{-1}\\&\quad x_{mi}(0,1)x_{jm}(0,s)x_{mi}(0,1)^{-1}x_{jm}(0,s)^{-1}\end{aligned}$$

但由(iii)知 $x_{ij}(r,0)^{-1}\underset{(S_1)}{=\!=}x_{ij}(-r,0)$ 与 $x_{mi}(0,-1)=x_{mi}(0,1)^{-1}$ 及 $x_{mi}(0,1)$ 对乘法是可交换的。由(ii)知 $x_{ij}(-r,0)$ 与 $x_{jm}(0,-s)=x_{jm}(0,s)^{-1}$ 及 $x_{jm}(0,s)$ 是乘法可交换的，由此知 $y=1$。

再证 $\mathrm{St}(R)\cap\mathrm{St}(S)=1$（在 $\mathrm{St}(R\oplus S)$ 中）。

任取 $\alpha\in\mathrm{St}(R)\cap\mathrm{St}(S)$。由上段证明可设 $\alpha=\alpha_1\alpha_2$，$\alpha_1\in\mathrm{St}(R)$，$\alpha_2\in\mathrm{St}(S)$。由 $\alpha,\alpha_1\in\mathrm{St}(R)$ 知 $\alpha_2\in\mathrm{St}(R)\cap\mathrm{St}(S)$，同理知 $\alpha_1\in\mathrm{St}(R)\cap\mathrm{St}(S)$。因此在 α 的下述不可缩短表示式

$$\alpha = x_{i_1j_1}(r_1,s_1)\cdots x_{i_tj_t}(r_t,s_t)$$

中可取 $\alpha_1 = x_{i_1j_1}(r_1,0)\cdots x_{i_tj_t}(r_t,0)$，$\alpha_2 = x_{i_1j_1}(0,s_1)\cdots x_{i_tj_t}(0,s_t)$ 使 $\alpha_1,\alpha_2 \in \mathrm{St}(R)\cap\mathrm{St}(S)$。因此 $r_1=\cdots=r_t=0$，$s_1=\cdots=s_t=0$，故由上知 $x_{i_lj_l}(r_l,s_l)=x_{i_lj_l}(0,0)=1$。因此 $\alpha=1$，即 $\mathrm{St}(R)\cap\mathrm{St}(S)=1$。

（2）由（1）知有群同态交换图

$$\begin{array}{ccc} \mathrm{St}(R\oplus S) & \xrightarrow{\simeq} & \mathrm{St}(R)\oplus\mathrm{St}(S) \\ \downarrow \phi_{R\oplus S} & & \downarrow \phi_R\oplus\phi_S \\ \mathrm{GL}(R\oplus S) & \xrightarrow[\simeq]{} & \mathrm{GL}(R)\oplus\mathrm{GL}(S) \end{array}$$

因此

$$\mathrm{K}_2(R\oplus S) = \mathrm{Ker}\phi_{R\oplus S} \simeq \mathrm{Ker}(\phi_R\oplus\phi_S) = \mathrm{K}_2(R)\oplus\mathrm{K}_2(S) \qquad \square$$

在上述证明中（事实上在命题10.2之证中）已得。

推论 10.1 $\forall R\in\mathcal{R}$ing，在 $\mathrm{St}(R)$ 中，$x_{ij}(0)=1$，$x_{ij}(a)^{-1}=x_{ij}(-a)$，$\forall a\in R$，$\forall i\neq j$。

定理 10.4 $\forall R\in\mathcal{R}$ing，$\forall n$，$\mathrm{K}_2(R^{n\times n})\simeq\mathrm{K}_2(R)$（$\mathrm{K}_2$ 群的弱 Morita 不变性）。

证 用分块矩阵法知 $\mathrm{GL}(R^{n\times n})\simeq\mathrm{GL}(R)$。而 $\mathrm{E}(S)=[\mathrm{GL}(S),\mathrm{GL}(S)]$，$\forall S\in\mathcal{R}$ing 时（命题5.2），因此 $\mathrm{E}(R^{n\times n})\simeq\mathrm{E}(R)$。再用下节将证的：$\mathrm{K}_2(S)$ 为 $\mathrm{E}(S)$ 的泛中心扩张之核及泛中心扩张的同构惟一性即得

$$\mathrm{K}_2(R^{n\times n})\simeq\mathrm{K}_2(R) \qquad \square$$

由上，我们得半单 Artin 环 K_2 群的下述结果。

推论 10.2 设 R 为半单 Artin 环，即

$$R\simeq D_1^{n_1\times n_1}\oplus\cdots\oplus D_k^{n_k\times n_k}, D_j \text{ 为除环}, j=1,\cdots,k$$

则

$$\mathrm{K}_2(R)\simeq\mathrm{K}_2(D_1)\oplus\cdots\oplus\mathrm{K}_2(D_k)$$

因此半单 Artin 环的 K_2 群的研究可归为除环的 K_2 群的研究。

由定理5.7又可得

定理 10.5 设有环同态 $f:R\to S$ 与 $g:S\to R$ 使 $gf=I_R$，则

（1）$\mathrm{K}_2(f)$ 为单同态，因此在同构意义下，$\mathrm{K}_2(R)$ 为 $\mathrm{K}_2(S)$ 的子群，即 $\mathrm{K}_2(R)\lesssim\mathrm{K}_2(S)$；

（2）$\mathrm{K}_2(g)$ 为满同态，因此 $\mathrm{K}_2(R)$ 又是 $\mathrm{K}_2(S)$ 的商群（同态象）；

（3）$\mathrm{K}_2(S)\simeq\mathrm{K}_2(R)\oplus\mathrm{Ker}\mathrm{K}_2(g)=\mathrm{Im}\mathrm{K}_2(g)\oplus\mathrm{Ker}\mathrm{K}_2(g)$。

推论 10.3 $\forall R\in\mathcal{R}$ing，

$$K_2(R[x_1,\cdots,x_n]) \simeq K_2(R) \oplus \mathrm{Ker}K_2(g),$$

其中 $g:R[x_1,\cdots,x_n]\to R$ 为使 $g(h(x_1,\cdots,x_n))=h(0,\cdots,0)$ 的环同态。

推论 10.4　设 $R\in \mathbb{R}\mathrm{ing}$，$G$ 为群，则

$$K_2(RG) \simeq K_2(R) \oplus \mathrm{Ker}K_2(g),$$

其中 $g:RG\to R$ 为使 $g(\Sigma r_jg_j)=\Sigma r_j$ 的环同态。

K_2 群的计算十分困难，但由其定义知，只要可以找出 $\mathrm{St}(R)$ 的元素 x 使 $\phi(x)=I$ 即可知 $x\in K_2(R)$。此法常有助于 K_2 群的研究与计算。

例 1　$\forall R\in \mathbb{R}\mathrm{ing}$，$e_{12}^{1}e_{21}^{-1}e_{12}^{1}=\mathrm{diag}\left(\begin{pmatrix} & 1\\ -1 & \end{pmatrix}, I_\infty\right)$，$\begin{pmatrix} & 1\\ -1 & \end{pmatrix}$在 $\mathbb{R}^2$ 中相当于旋转 90°的变换。令

$$x = (x_{12}(1)x_{21}(-1)x_{12}(1))^4$$

则

$$\phi(x)=\left(\begin{pmatrix}1 & 1 & \\ & 1 & \\ & & I_\infty\end{pmatrix}\begin{pmatrix}1 & & \\ -1 & 1 & \\ & & I_\infty\end{pmatrix}\begin{pmatrix}1 & 1 & \\ & 1 & \\ & & I_\infty\end{pmatrix}\right)^4$$

$$=\begin{pmatrix} & 1 & \\ -1 & & \\ & & I_\infty\end{pmatrix}^4 = I$$

于是 $x\in K_2(R)$，因此 $x\in C(\mathrm{St}(R))$。

在 $R=\mathbb{Z}$ 时，以后将证 $\mathrm{ord}x=2$ 且 $K_2(\mathbb{Z})=\langle x\rangle=\{1,x\}\simeq\mathbb{Z}_2$。

在 K_2 群的计算中，有时也需要将 $\mathrm{St}(R)$的一些子群排除在 $K_2(R)$之外（即找出 $\mathrm{St}(R)$的子群 N 使 $K_2(R)\cap N=1$）。比如，在命题 10.2 中，事实上已证 $K_2(R)\cap \mathbb{C}_n=K_2(R)\cap \mathbb{E}_n=1$。现在我们再证如下结果。

命题 10.3　$\forall R\in \mathbb{R}\mathrm{ing}$，记 $\mathrm{St}(R)$的子群

$$T = T(R) = \langle\{x_{ij}(a) \mid i<j,a\in R\}\rangle$$

$$T' = T'(R) = \langle\{x_{ij}(a) \mid i>j,a\in R\}\rangle$$

则 $K_2(R)\cap T=1$，$K_2(R)\cap T'=1$。

证　只需证 $T\cap K_2(R)=1$。事实上，$\forall \alpha_r=(a_1,\cdots,a_{r-1})^T\in R^{r-1}$，记

$$C_r(\alpha_r) = x_{1r}(a_1)x_{2r}(a_2)\cdots x_{r-1,r}(a_{r-1})$$

则 $T=\langle\{C_r(R^{r-1}),r=1,2,\cdots\}\rangle$。由 Steinberg 关系($S_2$)知，$\forall \beta_r=(b_1,\cdots,b_{r-1})^T\in R^{r-1}$

$$C_r(\alpha_r)C_r(\beta_r) = C_r(\alpha_r+\beta_r),$$

又由 Steinberg 关系(S_3)知，$\forall \beta_s=(b_1,\cdots,b_{s-1})^T\in R^{s-1}$，当 $r<s$ 时，视 $\alpha_r=$

$(\alpha_r,0,\cdots,0)\in R^{r-1}$（嵌入），则有

$$C_r(\alpha_r)C_s(\beta_s) = C_s(\beta_s + \alpha_r b_r)C_r(\alpha_r)$$

于是 $\forall t\in T$，必有 $\alpha_n,\cdots,\alpha_2$，其中 $\alpha_j\in R^{j-1}$，使

$$t = C_n(\alpha_n)C_{n-1}(\alpha_{n-1})\cdots C_2(\alpha_2)$$

但在 Steinberg 同态 ϕ: $\mathrm{St}(R)\to\mathrm{E}(R)$下，

$$\phi(t) = \begin{pmatrix} 1 & a_1 & \cdots & a_n \\ & \ddots & & \\ 0 & & & 1 \end{pmatrix} \in \mathrm{E}(R)$$

因此 $t\in T\cap \mathrm{K}_2(R)$时 $\alpha_j=0, j=1,2,\cdots$。再注意到 $C_j(0)=1$ 即知 $t=1$，即 $T\cap\mathrm{K}_2(R)=1$。 □

在§26 中，我们将给出 St(R)的一个子群 W＝W(R)使对 W 的任意元 w，$\phi(w)$都是单项矩阵（一置换矩阵与一对角矩阵之积），且 R 为除环时，St(R)＝TWT。这样，对 R 为域或除环的情况（$R^{\cdot}=R\backslash\{0\}$），就可断定 $W\subseteq \mathrm{K}_2(R)$，从而给出 $\mathrm{K}_2(R)$的全体生成元（生成系）。

§11　K_2 群的泛中心扩张刻画

在本节中我们来证明，环 R 的 K_2 群即 E(R)的泛中心扩张的核，这不仅从泛中心扩张角度刻画了 K_2 群，而且也补上了上节中证明 $\mathrm{K}_2(R^{n\times n})\simeq \mathrm{K}_2(R)$（$\mathrm{K}_2$ 群的弱 Morita 不变性）时缺少的一步。为此，需给出群论中的一个命题，作为本节的基础。

先回顾一下自由群的概念。

定义 11.1　设 X 为一个集合，F 是一个群，若有单射 $X\xrightarrow{i}F$（可看作 $X\subset F$）且具有如下泛性质：对任意群 H 与映射 $\varphi:X\to H$，必有惟一的群同态 $\psi:F\to H$ 使 $\psi i=\varphi$，即下图为交换图

$$\begin{array}{ccc} X & \xrightarrow{i} & F \\ {\scriptstyle\varphi}\downarrow & \swarrow {\scriptstyle \psi,\ \exists !} & \\ H & & \end{array}$$

则称 F 为以 X 作基的**自由群**（free group）。

显然，若有群的满同态 $\alpha:B\twoheadrightarrow C$ 与群同态 $\beta:F\to C$，则必有群同态 $\gamma:F\to B$ 使 $\alpha\gamma=\beta$。另一方面，任给群 G，以 G 的生成系$\{f_j\}$作基必得一自由群

F,且有显见的满同态 $F\twoheadrightarrow G$(使 F 的基元 $f_j\mapsto f_j$(G 的生成元)。因此,对任意的群 G,必有正合列 $1\to R\to F\to G\to 1$,其中 F 为自由群,此正合列称为 G 的**自由表示(现)**。

需注意的是自由 Abel 群 F_1(即 $F_1\in \mathrm{Free}_Z\mathfrak{M}$)一般地并非自由群,$F_1$ 的“自由性”是限制上述的 H 取自 Abel 群,而非取自任意群。事实上,自由群与自由 Abel 群都是“域上线性空间同态 $f:M\to N$ 由 M 之基元素在 f 下的象惟一确定”这一线性代数中的定理的不同程度的移植。

命题 11.1 (1)群 G 有泛中心扩张$\Leftrightarrow G$ 为完全群,即 $G=[G,G]$(例如非 Abel 单群);

(2) 群 G 的中心扩张(E,φ)为泛中心扩张$\Leftrightarrow$下两条成立:

(i) E 为完全群;

(ii) E 的中心扩张都是**平凡的(可裂的)**。即,设 $1\to B\to D\xrightarrow{\varphi'}\mathrm{E}\to 1$ 正合,(D,φ')为 E 的中心扩张,则$(D,\varphi')\simeq(\mathrm{E}\oplus B,p_1')$(其中 $\mathrm{E}\oplus B\underset{p_1}{\twoheadrightarrow}\mathrm{E}$ 为对第一直和项的标准投射)。即有群同构 $h:D\to \mathrm{E}\oplus B$ 使 $p_1'h=\varphi'$;

(3) 若 G 为完全群,

$$1\to R\to F\xrightarrow{\pi}G\to 1 \tag{1}$$

正合,其中 F 为自由群。则 G 的泛中心扩张(E,φ)可构作如下:取 $\mathrm{E}=[F,F]/[F,R]$,而 φ 即标准同态

$$[F,F]/[F,R]\xrightarrow{\varphi}[F,F]/R\simeq[F/R,F/R]\simeq[G,G]=G$$

证 (1)$\Rightarrow$:反设 G 不是完全群,记 $A=G/[G,G]\in \mathcal{A}G$,则 $A\neq 1$。令 $\pi':G\twoheadrightarrow A$ 为标准同态,显然 $G\oplus A\underset{p_1}{\twoheadrightarrow}G$ 为 G 的中心扩张(其中 p_1 为对第一直和项的标准投射)。任取$(\mathrm{E},\varphi)\in$ c. e. (G),下图中的 x 均有不同的两解 x_1,x_2。

$$\begin{array}{ccc} E & \xrightarrow{\varphi} & G \\ & \searrow^{x} & \uparrow{p_1} \\ & & G\oplus A \end{array}$$

其中,$x_1=(\varphi,1):y\mapsto(\varphi(y),1_A)$,这里 1_A 为 A 中的单位元,$x_2=(\varphi,\pi'\varphi)$:$y\mapsto(\varphi(y),\pi'\varphi(y))$,$\forall\, y\in \mathrm{E}$。因此 G 不可能有泛中心扩张。

$\Leftarrow$:设 G 为完全群,只需证下述两点(也同时证出了(2),(3))。

(a) G 的中心扩张若满足(2)中的(i),(ii),则必为泛中心扩张(因此(2)中$\Leftarrow$成立);

(b) (3)中的(E,φ)为满足(2)中的(i)(ii)的中心扩张,从而为 G 的泛中心扩张,于是 G 有泛中心扩张(因此(2)中的⇒与(3)成立)。

(a):设(E,φ)∈c. e(G)且满足(2)中的(i),(ii),(E_1,φ_1)∈c. e(G)。若有 ψ,ψ':(E,φ)→(E_1,φ_1)使 $\varphi_1\psi=\varphi=\varphi_1\psi'$,即 $\forall x\in \mathrm{E}$,

$$\varphi_1\psi(x)=\varphi(x)=\varphi_1\psi'(x)$$

于是有 $C_x\in \mathrm{Ker}\varphi_1\equiv A_1\subseteq C(\mathrm{E}_1)$使 $\psi(x)=C_x\psi'(x)$。同理 $\forall y\in \mathrm{E}$,有 $C_y\in A_1$ 使 $\psi(y)=C_y\psi'(y)$。但 $A_1\subseteq C(\mathrm{E}_1)$,因此

$$\begin{aligned}\psi([x,y])&=[\psi(x),\psi(y)]=[C_x\psi'(x),C_y\psi'(y)]\\&=[\psi'(x),\psi'(y)]=\psi'([x,y])\end{aligned}$$

而由(i),E=[E,E],于是 $\psi=\psi'$。下面再证 ψ 必存在,即得(a)。

令 $\mathrm{E}_2=\mathrm{E}\times_G\mathrm{E}_1\equiv\{(e_1,e_1)\in \mathrm{E}\times\mathrm{E}_1\mid\varphi(e)=\varphi_1(e_1)\}$(称为 E 与 E 在 G 上的纤维积,即后面 § 13 中的拉回图,亦称 Bear 和),则有交换图

$$\begin{array}{ccccc}
 & & E_2 & & \\
 & & \| & & \\
\mathrm{Ker}p_1\simeq 1\times\mathrm{Ker}\varphi_1 & \rightarrowtail & E\times_G E_1 & \overset{p_1}{\underset{i_1}{\rightleftarrows}} & E \\
 & & \downarrow p_2 & \swarrow \psi=p_2 i_1 & \downarrow \varphi \\
A_1=\mathrm{Ker}\varphi_1 & \rightarrowtail & E_1 & \xrightarrow{\varphi_1} & G
\end{array}\qquad(2)$$

其中 $p_1:(e,e_1)\mapsto e$,$p_2:(e,e_1)\mapsto e_1$,$\forall(e,e_1)\in\mathrm{E}_2$。

由 φ,φ_1 满知 p_1,p_2 满。又由 $\mathrm{Ker}p_1\simeq1\times\mathrm{Ker}\varphi_1$,$\mathrm{Ker}\varphi_1\subseteq C(\mathrm{E}_1)$,可知 $1\times\mathrm{Ker}\varphi_1\subseteq1\times C(\mathrm{E}_1)\subseteq C(\mathrm{E}\times_G\mathrm{E}_1)$,于是($\mathrm{E}_2$,$p_1$)∈c. e(E)。再由(ii)知($\mathrm{E}_2$,$p_1$)为 E 的平凡中心扩张。于是有 $i_1:\mathrm{E}\to\mathrm{E}_2$ 使 $p_1i_1=I_{\mathrm{E}}$. 由此知

$$\varphi_1p_2i_1=\varphi p_1i_1=\varphi$$

因此 $p_2i_1\equiv\psi$:(E,φ)→(E_1,φ_1)为中心扩张同态。即 ψ 存在,故(E,φ)∈u. c. e(G)。

(b):用(3)中的记号:E=[F,F]/[F,R],φ:E ↠[F,F]/$R\simeq G$。

由 $R\lhd F$ 知[F,R]⊆R($frf^{-1}r^{-1}\in Rr^{-1}=R$,$\forall f\in F,r\in R$),因此有 φ_1:

$$\mathrm{E}\subseteq\mathrm{E}_1\equiv F/[F,R]\xrightarrow[\varphi_1]{}F/R\simeq G\ 且\ \varphi=\varphi_1|_{\mathrm{E}}$$

但 $\mathrm{Ker}\varphi_1\subseteq R/[F,R]$。于是$[E_1,\mathrm{Ker}\varphi_1]\subseteq[F,R]/[F,R]=1$,因此 $\mathrm{Ker}\varphi_1\subseteq C(\mathrm{E}_1)$。注意到

$$\mathrm{Ker}\varphi\subseteq\mathrm{Ker}\varphi_1\subseteq C(\mathrm{E}_1)$$

知 $\mathrm{Ker}\varphi\subseteq \mathrm{E}\cap C(\mathrm{E}_1)\subseteq C(\mathrm{E})$，因此，$(\mathrm{E},\varphi)$，$(\mathrm{E}_1,\varphi_1)\in \mathrm{c.e}(G)$。下证$(\mathrm{E},\varphi)$满足(i)，(ii)即可。

(i) 事实上，由 E，E_1 的定义知，$\mathrm{E}=[E_1,\mathrm{E}_1]$。由 φ,φ_1 满且有交换图

$$\begin{array}{ccc} E & \xrightarrow{\varphi} & G \\ & \searrow \quad \nearrow_{\varphi_1} & \\ & E_1 & \end{array} \tag{3}$$

知 $\forall e_1\in \mathrm{E}_1, e\in \mathrm{E}$，若 $\varphi(e)=\varphi_1(e_1)$，注意 $\varphi=\varphi_1|_{\mathrm{E}}$，则有 $\varphi_1(e)=\varphi_1(e_1)$，于是 $e_1\in e\mathrm{Ker}\varphi_1$，因此 $\mathrm{E}_1=\langle \mathrm{E},\mathrm{Ker}\varphi_1\rangle$。但 $\mathrm{Ker}\varphi_1\subseteq C(\mathrm{E}_1)$，$\mathrm{E}\subseteq\mathrm{E}_1$，因此，$\mathrm{E}_1=\mathrm{E}\mathrm{Ker}\varphi_1\subseteq \mathrm{E}C(\mathrm{E}_1)$。由此知

$$\mathrm{E}=[\mathrm{E}_1,\mathrm{E}_1]\subseteq[\mathrm{E}C(\mathrm{E}_1),\mathrm{E}C(\mathrm{E}_1)]=[E,E]$$

即 E 为完全群，这就证出了(i)。

(ii) 令

$$1\to A_3\to \mathrm{E}_3\xrightarrow{\psi}\mathrm{E}\to 1 \tag{4}$$

为 E 的任一中心扩张（对应的正合列），证明其平凡（可裂）即可。

注意 $G=F/R\simeq[F,F]/R$，$\mathrm{E}=[F,F]/[F,R]\subseteq \mathrm{E}_1=F/[F,R]$。令 $\mathrm{E}_4=\mathrm{E}_1\times_G\mathrm{E}_3$，则有交换图（其中 π,π_1 为标准满同态，φ,φ_1 见(b)的证明，p_1，p_2 仿图(2)给出，ψ 即图(4)中的 ψ）。

$$\begin{array}{ccccc} & & F & & \\ & {\scriptstyle ②\theta}\swarrow & \downarrow{\scriptstyle ①h} & \searrow^{\pi_1} \quad \searrow^{\pi} & \\ & & E_4 & \xrightarrow{p_1} E_1 \ \ {\scriptstyle ④} & \\ & \swarrow_{p_2} \ {\scriptstyle ③\tilde\theta} & & \nearrow_{i} \quad \searrow_{\varphi_1} & \\ E_3 & \xrightarrow[\psi]{\ ⑤\theta_1\ } & E & \xrightarrow{\varphi} & G \end{array}$$

按下列顺序补图并证明(ii)。

①：由 F 的自由性与 p_1 为满同态知，有 h 使 $p_1h=\pi_1$；

②：取 $\theta=p_2h$；

③：由②与上图知，$\forall f\in F$，$\varphi\psi\theta(f)=\pi(f)$。因此

$$\theta(R)\xrightarrow[\varphi\psi]{}\pi(R)=\bar{1}$$

即，$\theta(R)\subseteq\mathrm{Ker}\varphi\psi$。下面证明

$$\mathrm{Ker}\varphi\psi\subseteq C(\mathrm{E}_3)$$

即知 $\theta(R)\subseteq C(\mathrm{E}_3)$，因此 $\theta(\mathrm{Ker}\pi_1)$为

$$\theta([F,R]) = [\theta(F),\theta(R)] \subseteq [E_3,C(E_3)] = 1$$

从而有 $\tilde{\theta}$ 使 $\tilde{\theta}\pi_1=\theta$。

事实上，由(b)中(i)之证知 E=[E,E]，因此

$$\psi([E_3,E_3]) = [\psi(E_3),\psi(E_3)] \underset{\psi\text{满}}{=\!=} [E,E] = E = \psi(E_3),$$

于是由 $A_3=\mathrm{Ker}\psi$ 知 $E_3=[E_3,E_3]A_3$。又由

$$\psi([E_3,\mathrm{Ker}\varphi\psi]) \subseteq [E,\mathrm{Ker}\varphi] \overset{c.e}{=\!=} 1$$

知

$$[E_3,\mathrm{Ker}\varphi\psi] \subseteq A_3 \underset{c.e}{\subset} C(E_3)$$

于是，$\forall x\in \mathrm{Ker}\varphi\psi, s,t\in E_3$，必有 $z_1,z_2\in C(E_3)$ 使

$$s^{-1}xsx^{-1} = z_1\text{，即 } xsx^{-1} = sz_1$$

$$t^{-1}xtx^{-1} = z_2\text{，即 } xtx^{-1} = tz_2$$

从而有

$$x[s,t]x^{-1} = [xsx^{-1},xtx^{-1}] = [sz_1,tz_2] \underset{z_i\in C(E_3)}{=\!=\!=\!=} [s,t]$$

即 x 与$[E_3,E_3]$中元素对乘法可交换。但 $x\in E_3$，$A_3\subseteq C(E_3)$，x 必与 A_3 中元素对乘法可交换，而由上知 $E_3=[E_3,E_3]A_3$，因此 $x\in C(E_3)$，故 $\mathrm{Ker}\varphi\psi\subseteq C(E_3)$。

④：来定义 λ 使 $p_1\lambda=I_{E_1}$。

$\forall f\in F,\pi_1(f)\equiv\bar{f}\in E_1$。由 $\tilde{\theta}\pi_1=\theta$，取 $\tilde{\theta}(\bar{f})=\theta(f)=e_3\in E_3$，则 $E_1=E_1\times_G E_3$ 的元素$(\bar{f},e_3)$使 $\varphi\psi(e_3)=\varphi_1(\bar{f})$。定义

$$\lambda: E_1 \to E_4$$

$$\bar{f} \mapsto (\bar{f},e_3)$$

则使 $p_1\lambda=I_{E_1}$。

⑤：限制 λ 到 E 上(此时 $\varphi=\varphi_1$)则对 $f_1,f_2\in F$，

$$\lambda(\overline{[f_1,f_2]}) = (\overline{[f_1,f_2]},e_3'),$$

其中 $\varphi\psi(e_3')=\varphi_1(\overline{[f_1,f_2]})$。由此知

$$p_2\lambda(\overline{[f_1,f_2]}) = \tilde{\theta}(\overline{[f_1,f_2]}) = e_3'$$

由上面的交换图，令 $\theta_1=\tilde{\theta}|_E: E\to E_3$，即得 $\psi\theta_1=I_E$。即，(E_3,ψ)为平凡(可裂)扩张。 □

由此命题可得

推论 11.1 群 G 有完全中心扩张(E,φ)(即满足 $E=[E,E]$的中心扩张(E,φ))$\Leftrightarrow G$ 有泛中心扩张。

证 $\Leftarrow$已由上证得到。

⇒：E 为完全群，且 φ 为满同态时 G 必为完全群。因此由上命题知 G 必有泛中心扩张。 □

下面来证明本节的主要结果：$(\mathrm{St}(R),\phi)\in$ u. c. e(E(R))。在上节，我们已知道：$(\mathrm{St}(R),\phi)\in$ c. e(E(R)) 且 St(R) 为完全群，因此满足命题 11.1 (2)中的(i)。现在只需证(ii)，即 St(R) 的任一中心扩张 (E,φ) 都是平凡的(可裂的)。为证此，先建立几条引理。

引理 11.1 设 $(E,\varphi)\in$ c. e(St(R))，$x,y\in \mathrm{St}(R)$，取 $X,Y\in E$ 使 $\varphi(X)=x,\varphi(Y)=y$，则 $[X,Y]$ 由 x,y 惟一确定而与 X,Y 的选取无关。因此，$[\varphi^{-1}(x),\varphi^{-1}(y)]$ 为 E 中的一个由 x,y 确定的元素。

证 若 $X_1,Y_1\in E$ 也使 $\varphi(X_1)=x,\varphi(Y_1)=y$，则有 $a_1,a_2\in \mathrm{Ker}\varphi\subseteq C(E)$ 使 $X=X_1a_1,Y=Y_1a_2$。于是 $[X,Y]=[X_1,Y_1]$。 □

由此引理知，可定义映射(注意 $[\mathrm{St}(R),\mathrm{St}(R)]=\mathrm{St}(R)$)

$$s:\mathrm{St}(R)\to E$$
$$[x,y]\mapsto[\varphi^{-1}(x),\varphi^{-1}(y)]$$

显然有 $\varphi s=I_{\mathrm{St}(R)}$，因此只需证 S 为群同态即可。为此给出

引理 11.2 $\forall j\neq k,i\neq l,a,b\in R$,

$$[\varphi^{-1}(x_{ij}(a)),\varphi^{-1}(x_{kl}(b))]=1\text{(E 中的单位元)。}$$

证 取 $h\neq i,j,k,l$。$u=\varphi^{-1}(x_{ih}(1))$，$v=\varphi^{-1}(x_{hj}(a))$，$w=\varphi^{-1}(x_{kl}(b))$。(这里的"="应为"∈"，由上引理知这样记法不影响下面的证明)。

由(S_3)知 $[u,v]\in\varphi^{-1}(x_{ij}(a))$。而由

$$\varphi([u,w])=[x_{ih}(1),x_{kl}(b)]=1$$
$$\varphi([v,w])=[x_{hj}(a),x_{kl}(b)=1,(S_2)$$

知 $[u,w],[v,w]\in \mathrm{Ker}\varphi\subseteq C(E)$，于是有 $c=[u,w]^{-1}=wuw^{-1}u^{-1}\in C(E)$，使 $ucw=cuw=wu$，因此 $cw=u^{-1}wu$。同理知有 $c'\in C(E)$ 使 $vc'w=c'vw=wv$。因此 $c'w=v^{-1}wv$。由此可算出

$$\begin{aligned}
&[\varphi^{-1}(x_{ij}(a)),\varphi^{-1}(x_{kl}(b))]\\
&=[[u,v],w]=(uvu^{-1}v^{-1})w(vuv^{-1}u^{-1})w^{-1}\\
&=(uvu^{-1})c'w(uv^{-1})(wu)^{-1}\\
&=c'uvu^{-1}w(uv^{-1})(w^{-1}u^{-1}c^{-1})\\
&=c'c^{-1}uv(cw)(w^{-1}v^{-1}(c')^{-1})u^{-1}\\
&=(uvw)(w^{-1}v^{-1}u^{-1})=1
\end{aligned}$$
□

引理 11.3 设 G 为任意群，$u,v,w\in G$，则

(1) $[u,v][u,w]=[u,vw][v,[w,u]]$;

(2) (Jacobi 恒等式)。若$[G,G]\in AG$,则

$$[u,[v,w]][v,[w,u]][w,[u,v]] = 1。$$

证 (1)直接验证即知。

(2):由(1)可得

$$[v,[w,u]] = [u,vw]^{-1}[u,v][u,w],$$
$$[u,[v,w]] = [w,uv]^{-1}[w,u][w,v],$$
$$[w,[u,v]] = [v,wu]^{-1}[v,w][v,u]。$$

由$[G,G]\in AG$及$[a,b][b,a]=1$即得

$$[u,[v,w]][v,[w,u]][w,[u,v]]$$
$$= [w,uv]^{-1}[w,u][w,v][u,vw]^{-1}[u,v][u,w]$$
$$[v,wu]^{-1}[v,w][v,u]$$
$$= (uvwv^{-1}u^{-1}w^{-1})(wuvu^{-1}w^{-1}v^{-1})(vwuw^{-1}v^{-1}u^{-1}) = 1$$ □

引理 11.4 设i,j,k,h互异,$a,b\in R$,则在 E 中

$$[\varphi^{-1}(x_{hj}(a)),\varphi^{-1}(x_{jk}(b))]$$
$$= [\varphi^{-1}(x_{hi}(1)),\varphi^{-1}(x_{ik}(ab))](\text{与 } j \text{ 无关})。 \tag{5}$$

证 由(S_3)知,在$\mathrm{St}(R)$中

$$[x_{hj}(a),x_{jk}(b)] = x_{hk}(ab) = [x_{hi}(1),x_{ik}(ab)]$$

取$u=\varphi^{-1}(x_{hi}(1)),v=\varphi^{-1}(x_{ij}(a)),w=\varphi^{-1}(x_{jk}(b))$,则有

$$[u,v] = \varphi^{-1}(x_{hj}(a)),\ [v,w] = \varphi^{-1}(x_{ik}(ab))$$

且(由引理 11.2)知,$[u,w]=1,[[u,v],u]=1,[[u,v],v]=1,[[u,v],[v,w]]=1$,记$G\equiv\langle\{u,v,w\}\rangle$,则由此知$[G,G]\in AG$。由引理 11.3 知:$[G,G]\in AG$时

$$[u,[v,w]][v,[w,u]][w,[u,v]] = 1$$

于是由$[w,u]=1$即知$[[u,v],w]=[u,[v,w]]$,从而即知本引理成立。 □

由这些引理可证明本节的主要结果。

定理 11.1 设$R\in\mathrm{Ring}$,则$(\mathrm{St}(R),\phi)\in$ u. c. e$(\mathrm{E}(R))$,因此$\mathrm{K}_2(R)$为$\mathrm{E}(R)$的泛中心扩张之核。

证 由引理 11.1 之前、后的分析知,只要证:对$\mathrm{St}(R)$的任一中心扩张(E,φ),

$$s:\mathrm{St}(R)\to \mathrm{E}$$
$$[x,y]\mapsto[\varphi^{-1}(x),\varphi^{-1}(y)] \tag{6}$$

(使$\varphi s=I_{\mathrm{St}(R)}$)为群同态即可。

为方便起见,在 E 中按引理 11.4 中(5)式右端(与i无关)记

$$s_{hk}(a) = [\varphi^{-1}(x_{hi}(1)), \varphi^{-1}(x_{ik}(a))] \in \varphi^{-1}(x_{hk}(a)),$$
$$\forall h \neq k, a \in R$$

由 φ 满且 $\mathrm{St}(R) = \langle\{x_{ij}(R) \mid i \neq j\}\rangle$ 知

$$\mathrm{E} = \langle\{s_{ij}(R) \mid i \neq j\}\rangle$$

下面只需证:对$\{s_{ij}(a)\}$,(S_1),(S_2),(S_3)成立,即知有确定同态

$$s: \mathrm{St}(R) \to \mathrm{E}$$
$$x_{ij}(a) \mapsto s_{ij}(a)$$

于是 $\varphi s = I_{\mathrm{St}(R)}$,且容易看出这个 s 正是上面(6)中的 s,于是定理即证出。

事实上,由引理 11.2 知(S_2)成立。由引理 11.4 容易看出(S_3)也成立。下证(S_1)成立,为此取 $a, b \in R$,k, i, j 互异,$u \in \varphi^{-1}(x_{ik}(1))$,$v \in \varphi^{-1}(x_{kj}(a))$,$w \in \varphi^{-1}(x_{kj}(b))$。则

$$\begin{aligned} s_{ij}(a)s_{ij}(b) &= [u,v][u,w] \\ &\xlongequal[\text{引理 } 11.3(1)]{} [u,vw][v,[w,u]] \\ &\xlongequal[\text{引理 } 11.2]{} [u,vw] = [\varphi^{-1}(x_{ik}(1)), \varphi^{-1}(x_{kj}(a+b))] \\ &\xlongequal[\text{定义}]{} s_{ij}(a+b) \end{aligned}$$

即(S_1)成立。 □

注①　在§1 例 1 中,我们给出了使 K_0 群平凡的例子,即设 V 为域 F 上无限维线性空间,$R = \mathrm{End}_F V$,证明了 $K_0(R) = 0$。下面我们证明对这个环 R,$K_1(R)$也是平凡的。

$\forall A, B \in \mathrm{GL}(R)$,记它们在 $K_1(R) = \mathrm{GL}(R)/\mathrm{E}(R)$中对应的元素为$[A]$,$[B]$,则$[A][B] = [AB]$,而

$$A \oplus B = \begin{pmatrix} A & \\ & B \end{pmatrix} = \begin{pmatrix} AB & \\ & I \end{pmatrix}\begin{pmatrix} B^{-1} & \\ & B \end{pmatrix}, \begin{pmatrix} B^{-1} & \\ & B \end{pmatrix} \in \mathrm{E}(R)$$

于是$[A \oplus B] = [AB \oplus I] = [AB] = [A][B]$。

注意由设知 $V \simeq \bigoplus_\infty V$,记$\bigoplus_\infty A \in \mathrm{GL}(R)$,则$[\bigoplus_\infty A] = [A \oplus (\bigoplus_\infty A)]$。又

$$[A][\bigoplus_\infty A] = [A \oplus (\bigoplus_\infty A)] = [\bigoplus_\infty A]$$

用群中的消去律即得$[A] = 1$,$\forall A \in \mathrm{GL}(R)$。故 $K_1(R) = 1$ 为平凡群。

还可证明对这个环 R,$K_2(R) = 1$ 也是平凡的。(见[Rosenberg,1994])这里不再介绍其证明。因为以后将更容易地证明:任何有限域 F_q 的 K_2 群都是平凡的。它们作为 K_2 群平凡的例子已足够丰富了。

§ 12 K_1 群与 K_2 群的同调刻画

设 G 为任一群(运算为乘法),则有整群环(也是$\mathbb{Z}$-代数)

$$\mathbb{Z}G = \left\{ \sum_{<\infty} n_j g_j \mid n_j \in \mathbb{Z}, g_j \in G \right\}$$

为简化记号,本节中的 $\sum$ 均表示有限和 $\sum_{<\infty}$。$\mathbb{Z}G$ 的加法、乘法为(其中的 m_i, n_j 可为 0)

$$\Sigma m_j g_j + \Sigma n_j g_j = \Sigma (m_j + n_j) g_j;$$

$$(\Sigma m_i g_i)(\Sigma n_j g_j) = \Sigma (m_i n_j)(g_i g_j)。$$

于是有环同态

$i: \mathbb{Z} \to \mathbb{Z}G$,

$n \mapsto ne$,其中 e 为 G 的单位元(常记 ne 为 n,$1e$ 为 1)

$\varepsilon: \mathbb{Z}G \to \mathbb{Z}$,

$\Sigma n_j g_j \mapsto \Sigma n_j$

在上述同态下,$\mathbb{Z}G \in {}_{\mathbb{Z}}\mathfrak{M}$(模运算为 $n(\Sigma n_j g_j) = \Sigma (nn_j) g_j$)且 $\mathbb{Z}G$ 为以 G 元素作基的自由$\mathbb{Z}$-模. $\mathbb{Z} \in {}_{\mathbb{Z}G}\mathfrak{M}$(模运算为 $(\Sigma n_j g_j) n = (\Sigma n_j) n$),又显然可以看出:$i$ 为单同态,ε 为满同态,$\mathbb{Z}$ 也是右$\mathbb{Z}G$-模。

记 $\mathfrak{g} = \mathrm{Ker}\varepsilon \equiv IG$(或 $I(\mathbb{Z}G)$,$\mathbb{Z}G$ 的理想),则有${}_{\mathbb{Z}G}\mathfrak{M}$ 中的正合列

$$0 \to \mathfrak{g} \to \mathbb{Z}G \xrightarrow{\varepsilon} \mathbb{Z} \to 0 \tag{1}$$

它作为${}_{\mathbb{Z}}\mathfrak{M}$ 中的正合列是可裂的(因为 $\varepsilon i = I_{\mathbb{Z}}$),但在${}_{\mathbb{Z}G}\mathfrak{M}$ 中一般地不是可裂的(因为一般地 i 不是${}_{\mathbb{Z}G}\mathfrak{M}$ 同态)。

定义 12.1 称 $\mathrm{Ker}\varepsilon = \mathfrak{g}$ 为$\mathbb{Z}G$ 的**增广理想**(augmentation ideal)。

注意到$\mathbb{Z} \in$ PID,自由$\mathbb{Z}$-模之子模仍为自由$\mathbb{Z}$-模可知 $\mathfrak{g} \in \mathrm{Free}_{\mathbb{Z}}\mathfrak{M}$。事实上,也可直接证明更强的下述结果:

命题 12.1 设 G 为群,$g \in G$,则 $g - 1 \in \mathfrak{g}$($\mathbb{Z}G$ 的增广理想)且

$$W \equiv \{g - 1 \mid g \neq e, g \in G\}$$

为 $\mathfrak{g} \in \mathrm{Free}_{\mathbb{Z}}\mathfrak{M}$ 之基。

证 显然 W 为$\mathbb{Z}$-线性无关的。只需再证 W 生成 $\mathfrak{g}$。

任取 $\Sigma n_j g_j \in \mathfrak{g}$,则由 $\mathfrak{g}$ 的定义知 $\Sigma n_j = 0$。于是

$$\Sigma n_j (g_j - 1) = \Sigma n_j g_j$$

即,W 为 $\mathfrak{g}$ 的$\mathbb{Z}$-生成系。故 W 为 $\mathfrak{g} \in \mathrm{Free}_{\mathbb{Z}}\mathfrak{M}$ 的基。 □

注①　当 G 为自由群,其基为 X 时,$\mathrm{g}\in \mathrm{Free}_{\mathbb{Z}G}\mathfrak{M}$,其基为 $\{x-1 \mid x\in X\}$(见[Suzuki,1982])。

定义 12.2　设 G 为群,记

$$\mathrm{H}_n(G,-)=\mathrm{Tor}_n^{\mathbb{Z}G}(\mathbb{Z},-)$$

称为 G 的第 n 个**同调函子**。对 $\forall M\in {}_{\mathbb{Z}G}\mathfrak{M}$,称 $\mathrm{H}_n(G,M)=\mathrm{Tor}_n^{\mathbb{Z}G}(\mathbb{Z},M)$ 为 G 的系数在 M 中的第 n 个**同调群**(常取 $M=\mathbb{Z}$)。记

$$\mathrm{H}^n(G,-)=\mathrm{Ext}_{\mathbb{Z}G}^n(\mathbb{Z},-)$$

称为 G 的第 n 个**上同调函子**,对 $\forall M\in {}_{\mathbb{Z}G}\mathfrak{M}$,称 $\mathrm{H}^n(G,M)=\mathrm{Ext}_{\mathbb{Z}G}^n(\mathbb{Z},M)$ 为 G 的系数在 M 中的第 n 个**上同调群**。

这些都是常用的 G 的同调不变量(见[佟文廷,1998])。本节中我们只介绍用以刻画 K_1 群、K_2 群的同调群,用到的同调工具可参看[佟,1998]。先证明一条关于 $\mathrm{H}_1(G,\mathbb{Z})$ 的引理。

引理 12.1　设 G 为群,则

$$\mathrm{H}_1(G,\mathbb{Z})\simeq \mathrm{H}_0(G,\mathrm{g})\simeq \mathbb{Z}\bigotimes_{\mathbb{Z}G}\mathrm{g},$$

$$\mathrm{H}_2(G,\mathbb{Z})\simeq \mathrm{H}_1(G,\mathrm{g})=\mathrm{Tor}_1^{\mathbb{Z}G}(\mathbb{Z},\mathrm{g})。$$

证　以 $\mathbb{Z}\bigotimes_{\mathbb{Z}G}-$ 作用于(1),由长正合列定理得正合列(其中 ∂ 为连接同态),$\mathrm{H}_2(\mathbb{Z},G\mathbb{Z})\to \mathrm{H}_2(G,\mathbb{Z})\xrightarrow{\partial}\mathrm{H}_1(G,\mathrm{g})\to \mathrm{H}_1(G,\mathbb{Z}G)\to \mathrm{H}_1(G,\mathbb{Z})\xrightarrow{\partial}$ $\mathrm{H}_0(G,\mathrm{g})\to \mathrm{H}_0(G,\mathbb{Z}G)\xrightarrow{\varepsilon_*}\mathrm{H}_0(G,\mathbb{Z})\to 0$。由 $\mathbb{Z}G$ 为投射 $\mathbb{Z}G$ 模知,$\mathrm{H}_j(G,\mathbb{Z}G)=0$,$j=1,2$。因此 $\mathrm{H}_2(G,\mathbb{Z})\simeq \mathrm{H}_1(G,\mathrm{g})=\mathrm{Tor}_1^{\mathbb{Z}G}(\mathbb{Z},\mathrm{g})$。又

$$\mathrm{H}_0(G,\mathrm{g})\simeq \mathbb{Z}\bigotimes_{\mathbb{Z}G}\mathrm{g},$$

$$\mathrm{H}_0(G,\mathbb{Z}G)\simeq \mathbb{Z}\bigotimes_{\mathbb{Z}G}\mathbb{Z}G\simeq \mathbb{Z},$$

$$\mathrm{H}_0(G,\mathbb{Z})\simeq \mathbb{Z}\bigotimes_{\mathbb{Z}G}\mathbb{Z}\simeq \mathbb{Z}$$

(注意 $\varepsilon_*=I_Z\otimes\varepsilon$ 为满同态,$\mathrm{Im}\varepsilon_*\simeq\mathbb{Z}$)。

但 $\mathbb{Z}$ 的自同态或为同构或为零同态,因此 ε_* 为同构。于是 $\mathrm{Ker}\varepsilon_*=0$。由此知道有正合列

$$0\to \mathrm{H}_1(G,\mathbb{Z})\xrightarrow{\partial}\mathrm{H}_0(G,\mathrm{g})\to 0$$

故

$$\mathrm{H}_1(G,\mathbb{Z})\simeq \mathrm{H}_0(G,\mathrm{g})\simeq \mathbb{Z}\bigotimes_{\mathbb{Z}G}\mathrm{g}$$ □

注②　尽管在(1)中 $\varepsilon i=I_Z$,但一般地,i 非 ${}_{\mathbb{Z}G}\mathfrak{M}$ 中的同态。因此,一般地 $\mathbb{Z}$ 不是投射 $\mathbb{Z}G$-模。可以证明:当 $|G|<\infty$ 且 $|G|$ 在 R 中可逆时(即 $|G|\in R^{\cdot}$),$R\in \mathrm{P}_{RG}\mathfrak{M}$。且 $Q\in \mathrm{P}_R\mathfrak{M}$ 时 $Q\in \mathrm{P}_{RG}\mathfrak{M}$(见[Karpilovsky,1983])。

由上引理，我们可证 $H_1(G,\mathbb{Z})$ 事实上即 G 的 Abel 化 G^{ab}。即

命题 12.2 设 G 为群，则

$$H_1(G,\mathbb{Z}) \simeq \mathbb{Z} \underset{\mathbb{Z}G}{\otimes} \mathfrak{g} \simeq \mathfrak{g}/\mathfrak{g}^2 \simeq G^{ab} \equiv G/[G,G]$$

因此，(1)若 $G\in\mathcal{A}G$，则 $H_1(G,\mathbb{Z})\simeq G$，(2)$G$ 为完全群$\Leftrightarrow H_1(G,\mathbb{Z})=1$ 为平凡的。

证 由引理 12.1 知，只需证

$$\mathbb{Z} \underset{\mathbb{Z}G}{\otimes} \mathfrak{g} \simeq \mathfrak{g}/\mathfrak{g}^2 \simeq G^{ab}$$

以 $-\underset{\mathbb{Z}G}{\otimes}\mathfrak{g}$ 作用于(1)得正合列

$$\mathfrak{g}\underset{\mathbb{Z}G}{\otimes}\mathfrak{g} \xrightarrow{\tau} \mathbb{Z}G \underset{\mathbb{Z}G}{\otimes}\mathfrak{g} \xrightarrow{\varepsilon\otimes I} \mathbb{Z}\underset{\mathbb{Z}G}{\otimes}\mathfrak{g} \to 0$$

$$\mathbb{Z}G \underset{\mathbb{Z}G}{\otimes}\mathfrak{g} \simeq \mathfrak{g}$$

由此知

$$\mathbb{Z} \underset{\mathbb{Z}G}{\otimes} \mathfrak{g} \simeq (\mathbb{Z}G \underset{\mathbb{Z}G}{\otimes} \mathfrak{g})/\mathrm{Im}\tau \simeq \mathfrak{g}/\mathfrak{g}^2$$

又由命题 12.1 知，$\forall e\neq g\in G, g-1\in\mathfrak{g}=\mathrm{Ker}\varepsilon$，于是由

$$\begin{aligned}&(xy-1)-(x-1)-(y-1)\\ &=(x-1)(y-1)\in\mathfrak{g}^2,\ \forall x,y\in G\end{aligned}$$

即

$$xy-1\equiv(x-1)+(y-1) \bmod \mathfrak{g}^2$$

可定义群同态

$$\begin{aligned}\theta: G &\to \mathfrak{g}/\mathfrak{g}^2,\\ g &\mapsto (g-1)+\mathfrak{g}^2\end{aligned}$$

由

$$\begin{aligned}\theta([g_1,g_2]) &= (g_1-1)+(g_2-1) \quad -(g_1-1)-(g_2-1)+\mathfrak{g}^2\\ &= \mathfrak{g}^2 \equiv 0 \bmod \mathfrak{g}^2\end{aligned}$$

知，$[G,G]\subseteq\mathrm{Ker}\theta$。于是 θ 诱导出满同态

$$\begin{aligned}\tilde{\theta}: G^{ab} &\twoheadrightarrow \mathfrak{g}/\mathfrak{g}^2\\ g[G,G] &\mapsto (g-1)+\mathfrak{g}^2\end{aligned}$$

下面证 $\tilde{\theta}$ 为同构即可。

事实上，定义 Abel 群同态

$$\begin{aligned}\varphi: \mathfrak{g} &\to G^{ab}\\ g-1 &\mapsto g[G,G]\end{aligned}$$

注意 $\forall u\in\mathfrak{g}^2$，

$$u=\sum m_i n_j(x_i-1)(y_j-1)$$

$$= \Sigma m_i n_j [(x_i y_j - 1) - (x_i - 1) - (y_j - 1)]$$

$$\varphi(u) = \prod [x_i, y_j]^{m_i n_j} [G,G] \subseteq [G,G]$$

则知 $\mathfrak{g}^2 \subseteq \mathrm{Ker}\varphi$。于是 φ 诱导出同态

$$\tilde{\varphi}: \mathfrak{g}/\mathfrak{g}^2 \to G^{ab}$$

可直接验证：$\tilde{\varphi}\theta = I_{G^{ab}}$，$\theta\tilde{\varphi} = I_{\mathfrak{g}/\mathfrak{g}^2}$。故 θ 为同构。 □

由命题 12.2 立得 K_1 群的下述同调刻画。

定理 12.1　$\forall R \in \mathcal{R}\mathrm{ing}$，

$$K_1(R) = \mathrm{GL}(R)^{ab} \simeq H_1(\mathrm{GL}(R), \mathbb{Z})$$

下面再来讨论 K_2 群的同调刻画。

如众周知，对任意的 Abel 群 A，A 的自同态集 $\mathrm{End}A$（即 $\mathrm{End}_{\mathbb{Z}}A$）按下面定义的运算（设 A 为乘法群，加法群可类似地定义）

$$(\alpha\beta)(a) = \alpha(\beta(a))$$

$$(\alpha + \beta)(a) = \alpha(a)\beta(a), \quad \forall \alpha, \beta \in \mathrm{End}A, a \in A$$

$$(\alpha - \beta)(a) = \alpha(a)\beta(a)^{-1}$$

成一环，且使 $A \in {}_{\mathrm{End}_A}\mathfrak{M}$（$\mathfrak{M}_{\mathrm{End}A}$）。对任一群 G，任取群同态

$$\sigma: G \to \mathrm{Aut}A\text{（}A\text{ 的自同构群）}$$

规定 $ga = \sigma(g)a$，$\forall g \in G, a \in A$，称 A 为 G-模（关于 σ），记为 $A \in {}_G\mathfrak{M}$，$\sigma(G) = I_A$ 时称 G 平凡作用于 A。由于 σ 必诱导（可开拓为）一个环同态 $\sigma': \mathbb{Z}G \to \mathrm{End}A$ 使 $\sigma'|_G = \sigma$。因此由 $A \in {}_{\mathrm{End}_A}\mathfrak{M}$ 知 $A \in {}_{\mathbb{Z}G}\mathfrak{M}$。反过来，若 $A \in {}_{\mathbb{Z}G}\mathfrak{M}$，注意 σ' 保持可逆元对应，即 $\sigma'(\mathbb{Z}G)^{\cdot} \subseteq \mathrm{Aut}A$。而 $G \subseteq (\mathbb{Z}G)^{\cdot}$，于是 $A \in {}_G\mathfrak{M}$。因此，可以认为 ${}_{\mathbb{Z}G}\mathfrak{M} = {}_G\mathfrak{M}$。于是有

引理 12.2　设 G 为群，A 为 Abel 群，则对任意的群同态 $\sigma: G \to \mathrm{Aut}A$，$A \in {}_{\mathbb{Z}G}\mathfrak{M} = {}_G\mathfrak{M}$。

由上节命题 11.1 及证明中的(b)，我们已经得到

命题 12.3　设 G 为任一群，则

(1) 必有群的自由表现（群同态正合列）

$$1 \to R \to F \xrightarrow{\pi} G \to 1, \tag{2}$$

其中 F 为自由群（比如可取为以 G 的生成系作基的自由群）且 $[F,R] \lhd F$；

(2) 令 $E_1 = F/[F,R]$，π 诱导的群满同态 $\varphi_1: E_1 \to G \simeq F/R$，则 $(E_1, \varphi_1) \in \mathrm{c.e}(G)$；

(3) 令 $E = [F,F]/[F,R]$，$\varphi = \varphi_1|_E$，则当 G 为完全群时 $(E,\varphi) \in \mathrm{u.c.e}(G)$。

不难证明如下结果：

命题 12.4 设 G 为完全群，则在命题 12.3 的记号下，G 的泛中心扩张 (E,φ) 之核

$$\mathrm{Ker}\varphi \simeq (R\cap[F,F])/[F,R]$$

证 注意 G 的泛中心扩张在同构意义下是惟一的，由标准同态

$$[F,F]/[F,R]=E \underset{\varphi}{\twoheadrightarrow} F/R\simeq G$$

即得证。 □

注③ 泛中心扩张是 1904 年首次由 J. Schur（对有限群）引进的，因此常称 $(R\cap[F,F])/[F,R]$ 为 G 的 Schur 乘子（multiplier）。

下面为证明本节的另一个关键性结果—Hopf 公式（H. Hopf，1894－1971），先证几条引理。

引理 12.3 设群 G 的自由表现为(2)中所示，则

$$\mathbb{Z}\underset{\mathbb{Z}G}{\otimes}R^{ab}\simeq R/\mathrm{g}R\simeq R/[F,R]$$

其中 g 为 $\mathbb{Z}G$ 的增广理想（即(1)中的 $\mathrm{Ker}\varepsilon$）。

证 由于 $R^{ab}\in{}_{\mathbb{Z}}G$，由引理 12.2 知 $R^{ab}\in{}_{\mathbb{Z}G}\mathfrak{M}$，以右正合函子 $-\underset{\mathbb{Z}G}{\otimes}R^{ab}$ 作用于(1)得正合列

$$\begin{array}{c}\mathrm{g}\underset{\mathbb{Z}G}{\otimes}R^{ab}\xrightarrow{\tau}\mathbb{Z}G\underset{\mathbb{Z}G}{\otimes}R^{ab}\to\mathbb{Z}\underset{\mathbb{Z}G}{\otimes}R^{ab}\to 0\\ \wr\|\\ R^{ab}\end{array}$$

由此知

$$\begin{aligned}\mathbb{Z}\underset{\mathbb{Z}G}{\otimes}R^{ab}&\simeq R^{ab}/\mathrm{Im}\tau=R^{ab}/\mathrm{g}R^{ab}\\ &\simeq(R/[R,R])/(\mathrm{g}R/[R,R])\simeq R/\mathrm{g}R\end{aligned}\tag{3}$$

在 G 的自由表现(2)中，$\forall g\in G$，必有 $f\in F$ 使 $\pi(f)=g$，而由命题 12.1 知

$$\begin{aligned}\mathrm{g}R^{ab}&=\langle\{(g-1)r[R,R]\mid \begin{smallmatrix}r\in R\\ e\neq g\in G\end{smallmatrix}\}\rangle\\ &=\langle\{(g-1)\bar{r}\mid \begin{smallmatrix}r\in R\\ e\neq g\in G\end{smallmatrix}\}\rangle\end{aligned}$$

取引理 12.2 之推证中的 σ 为（注意 $R\lhd F$）$\sigma:G\to\mathrm{Aut}R^{ab}$ 使 $\sigma(g)\in\mathrm{Aut}R^{ab}$，而 $\sigma(g)(\bar{r})=f\bar{r}f^{-1}$（这里的 $f\in\pi^{-1}(g)\subseteq F$，即 $\pi(f)=g$）。开拓 σ 为环同态

$$\sigma':\mathbb{Z}G\to\mathrm{End}R^{ab}$$

则 $R^{ab}\in{}_{\mathbb{Z}G}\mathfrak{M}$（通过 σ'）。于是由

$$\begin{aligned}\sigma'(g-1)(\bar{r})=(\sigma(g)-\sigma(e_G))(\bar{r})&=f\bar{r}f^{-1}(1_F\bar{r}1_F^{-1})^{-1}\\ &=frf^{-1}r^{-1}[R,R]\in[F,R]/[R,R]\end{aligned}$$

知，

$$gR/[R,R] = R^{ab} = gR^{ab}[F,R]/[R,R]$$

因此 $gR \simeq [F,R]$。故

$$\mathbb{Z} \underset{\mathbb{Z}G}{\otimes} R^{ab} \underset{(3)}{\widetilde{=}} R/gR \simeq R/[F,R] \qquad \square$$

由引理 12.1 已知 $H_2(G,\mathbb{Z}) \simeq H_1(g,\mathbb{Z})$。为研究 $H_2(G,\mathbb{Z})$，需考察 g 的 $P_{\mathbb{Z}G}\mathfrak{M}$ 分解，为此再证

引理 12.4　在(2)中记号下，令

$$0 \to \mathscr{F} \to \mathbb{Z}F \to \mathbb{Z} \to 0 \tag{4}$$

为 $_{\mathbb{Z}F}\mathfrak{M}$ 正合列(即 $\mathscr{F}$ 为 $\mathbb{Z}F$ 的增广理想)，则有 $_{\mathbb{Z}G}\mathfrak{M}$ 正合列

$$0 \to R^{ab} \to \mathbb{Z}G \underset{\mathbb{Z}F}{\otimes} \mathscr{F} \to g \to 0 \tag{5}$$

证　以 $\mathbb{Z}G \underset{\mathbb{Z}F}{\otimes} -$ (注意由(2)知 $\mathbb{Z}G \in {}_{\mathbb{Z}F}\mathfrak{M}$)作用于(4)。由长正合列定理知，有正合列

$$\begin{array}{ccccccccc}
\mathrm{Tor}_1^{\mathbb{Z}F}(\mathbb{Z}G,\mathbb{Z}F) & \longrightarrow & \mathrm{Tor}_1^{\mathbb{Z}F}(\mathbb{Z}G,\mathbb{Z}) & \to & \mathbb{Z}G \underset{\mathbb{Z}F}{\otimes} \mathscr{F} & \to & \mathbb{Z}G \underset{\mathbb{Z}F}{\otimes} \mathbb{Z}F & \to & \mathbb{Z}G \underset{\mathbb{Z}F}{\otimes} \mathbb{Z} \to 0 \\
\| \ \mathbb{Z}F \in P_{\mathbb{Z}F}\mathfrak{M} & & \wr\ ② & & & & \wr & & \wr\ ① \\
0 & & R^{ab} & & & & & & \\
 & & & & 0 \longrightarrow g & \longrightarrow & \mathbb{Z}G & \longrightarrow & \mathbb{Z} \longrightarrow 0
\end{array}$$

只需证上图中的①，②即可。

①：G 的自由表现(2)中的 $\pi: F \to G$ 诱导出环同态

$$\pi': \mathbb{Z}F \to \mathbb{Z}G$$
$$\Sigma n_i f_i \mapsto \Sigma n_i \pi(f_i)$$

由此知 $\mathbb{Z}G$ 的 $_{\mathbb{Z}F}\mathfrak{M}$ 乘法运算事实上即 $\mathbb{Z}G$ 的乘法运算。而在 π' 之下，$\mathbb{Z}$ 作为 $_{\mathbb{Z}F}\mathfrak{M}$ 与作为 $_{\mathbb{Z}G}\mathfrak{M}$ 的乘法运算是一样的，即 $\forall\, n \in \mathbb{Z}$，

$$(\Sigma n_i f_i)n = (\Sigma n_i)n = (\Sigma n_i \pi(f_i))n$$

因此

$$\mathbb{Z}G \underset{\mathbb{Z}F}{\otimes} \mathbb{Z} \simeq \mathbb{Z}G \underset{\mathbb{Z}G}{\otimes} \mathbb{Z} \simeq \mathbb{Z}$$

②：由(2)中的 $R \lhd F$ 知 F 可写成 R 的(左)陪集之直并

$$F = \dot{\bigcup_{j\in J}} f_j R,\ f_j \in F, \text{可取 } J \text{ 使 } |J| = |G|。$$

对任意的 $j \in J$，$\mathbb{Z}F$ 中 $f_j R \mathbb{Z}$ 生成的 $\langle f_j R\rangle_{\mathbb{Z}} \simeq \mathbb{Z}R$。因此

$$\mathbb{Z}F \simeq \bigoplus_{j\in J} \mathbb{Z}R \in \mathrm{Free}_{\mathbb{Z}R}\mathfrak{M}$$

于是，$\forall\, X \in {}_{\mathbb{Z}F}\mathfrak{M}$ 的 $\mathbb{Z}F$-投射分解也是它的 $\mathbb{Z}R$-投射分解。而由 $|J| = |G|$ 又知

$$\mathbb{Z} \underset{\mathbb{Z}R}{\otimes} \mathbb{Z}F \simeq \mathbb{Z} \underset{\mathbb{Z}R}{\otimes} \Big(\bigoplus_{j\in J} \mathbb{Z}R\Big) \simeq \bigoplus_{j\in J} \mathbb{Z} \simeq \mathbb{Z}G,$$

$$\mathbb{Z} \underset{\mathbb{Z}R}{\otimes} X \simeq \mathbb{Z} \underset{\mathbb{Z}R}{\otimes} \mathbb{Z}F \underset{\mathbb{Z}F}{\otimes} X \simeq \mathbb{Z}G \underset{\mathbb{Z}R}{\otimes} X。$$

因此

$$\mathrm{Tor}_n^{\mathbb{Z}R}(\mathbb{Z},X) \simeq \mathrm{Tor}_n^{\mathbb{Z}F}(\mathbb{Z}G,X)$$

特别地,由命题 12.2 又得

$$\mathrm{Tor}_{1}^{\mathbb{Z}F}(\mathbb{Z}G,\mathbb{Z}) \simeq \mathrm{Tor}_1^{\mathbb{Z}R}(\mathbb{Z},\mathbb{Z}) \simeq R^{ab}$$ □

命题 12.5 (Hopf 公式) 设 G 为群,

$$1 \to R \to F \to G \to 1$$

为 G 的自由表现(即上列为正合列,其中 F 为自由群),则

$$\mathrm{H}_2(G,\mathbb{Z}) \simeq (R \cap [F,F])/[F,R],$$

因此右端与 F 的选取无关。

证 以 $\mathbb{Z}\underset{\mathbb{Z}G}{\otimes}$ 作用于引理 12.4 所得的正合列

$$0 \to R^{ab} \to \mathbb{Z}G \underset{\mathbb{Z}F}{\otimes} \mathscr{F} \to \mathrm{g} \to 0$$

由长正合列定理得正合列

$$\mathrm{Tor}_1^{\mathbb{Z}G}(\mathbb{Z},\mathbb{Z}G \underset{\mathbb{Z}F}{\otimes} \mathscr{F}) \to \mathrm{Tor}_1^{\mathbb{Z}G}(\mathbb{Z},\mathrm{g})$$

$$\to \mathbb{Z} \underset{\mathbb{Z}G}{\otimes} R^{ab} \xrightarrow{\lambda} \mathbb{Z} \underset{\mathbb{Z}G}{\otimes} \mathbb{Z}G \underset{\mathbb{Z}F}{\otimes} \mathscr{F}$$

由 $\mathbb{Z}G \in \mathrm{P}_{\mathbb{Z}G}\mathfrak{M}$ 及 F 为自由群所决定的 $\mathscr{F} \in \mathrm{Free}_{\mathbb{Z}F}\mathfrak{M}$ 知,$\mathbb{Z}G\underset{\mathbb{Z}F}{\otimes}\mathscr{F} \in \mathrm{P}_{\mathbb{Z}G}\mathfrak{M}$,因此 $\mathrm{Tor}_1^{\mathbb{Z}G}(\mathbb{Z},\mathbb{Z}G\underset{\mathbb{Z}F}{\otimes}\mathscr{F})=0$。又由引理 12.1 知 $\mathrm{Tor}_1^{\mathbb{Z}G}(\mathbb{Z},\mathrm{g}) \simeq \mathrm{H}_2(G,\mathbb{Z})$,由引理 12.3 知 $\mathbb{Z}\underset{\mathbb{Z}G}{\otimes}R^{ab} \simeq R/[F,R]$。再由命题 12.2 又知

$$\mathbb{Z} \underset{\mathbb{Z}G}{\otimes} \mathbb{Z}G \underset{\mathbb{Z}F}{\otimes} \mathscr{F} \simeq \mathbb{Z} \underset{\mathbb{Z}F}{\otimes} \mathscr{F} \simeq F^{ab}$$

故

$$\mathrm{H}_2(G,\mathbb{Z}) \simeq \mathrm{Ker}\lambda = (R \cap [F,F])/[F,R]$$ □

由命题 12.4 与命题 12.5 立得

命题 12.6 设 G 为完全群,则 G 的泛中心扩张之核同构于 $\mathrm{H}_2(G,\mathbb{Z})$。

最后由 $\mathrm{K}_2(R)$ 为 $\mathrm{E}(R)$ 的泛中心扩张之核得 $\mathrm{K}_2(R)$ 的同调刻画。

定理 12.2 设 $R \in \mathfrak{R}\mathrm{ing}$,则

$$\mathrm{K}_2(R) \simeq \mathrm{H}_2(\mathrm{E}(R),\mathbb{Z})$$

由命题 12.2 知,事实上,我们已证出:$\forall R \in \mathfrak{R}\mathrm{ing}$, $\mathrm{H}_1(\mathrm{St}(R),\mathbb{Z})=1$, $\mathrm{H}_1(\mathrm{E}(R),\mathbb{Z})=1$。

由 $\mathrm{K}_1(R)$, $\mathrm{K}_2(R)$ 的定义,我们已知有群正合列

$$\begin{array}{ccccc} 1 \to \mathrm{K}_2(R) \to \mathrm{St}(R) & \xrightarrow{\phi_1} & \mathrm{GL}(R) \to \mathrm{K}_1(R) \to 1 \\ \phi \searrow & & \nearrow \\ & \mathrm{E}(R) & \end{array}$$

对由 Quillen 的高阶 K-理论，用分类空间定义的 $K_3(R)$ 亦有相应的结果：

$$K_3(R) \simeq H_3(St(R), \mathbb{Z})$$

这是 1973 年 S. M. Gersten 在 Proc. Amer. Math. Soc. 366－368 发表的。此外，又可证明：有群的满同态

$$K_2(R) \twoheadrightarrow H_2(GL(R), \mathbb{Z}),$$
$$K_3(R) \twoheadrightarrow H_3(E(R), \mathbb{Z}),$$
$$K_4(R) \twoheadrightarrow H_4(St(R), \mathbb{Z})。$$

(见[Berrick，1982]、[周伯勋，1987])。

回顾一下上同调泛系数定理(见[佟文廷．1998])：设 R 为右遗传环(即 $rD(R) \leqslant 1$)。$(\mathscr{X}, d)$ 为投射右 R-模复形，$A \in \mathfrak{M}_R$，则有可裂正合列(可裂性未必自然)

$$0 \to \mathrm{Ext}_R^1(H_{n-1}(\mathscr{X}), A) \xrightarrow{\lambda} H^n(\mathrm{Hom}_R(\mathscr{X}, A))$$
$$\xrightarrow{\mu} \mathrm{Hom}_R(H_n(\mathscr{X}), A) \to 0, \ \forall n,$$

其中 λ, μ 都是自然的。

将此定理用于群 G，注意 $H_n(G, \mathbb{Z}) = \mathrm{Tor}_n^{\mathbb{Z}G}(\mathbb{Z}, \mathbb{Z})$ 为 $\mathbb{Z}$ 的 $\mathbb{Z}G$-模(删项)投射分解 $\mathscr{P}_{\hat{\mathbb{Z}}}$ 在 $-\otimes_{\mathbb{Z}G}\mathbb{Z}$ 作用下得到的复形 $\mathscr{P}_{\hat{\mathbb{Z}}}\otimes_{\mathbb{Z}G}\mathbb{Z}$ 的同调。$\mathscr{P}_{\hat{\mathbb{Z}}}\otimes_{\mathbb{Z}G}\mathbb{Z}$ 显然为投射 $\mathbb{Z}$-模复形。$\mathbb{Z}$ 当然为遗传环，于是对任意 Abel 群 A(即 $A \in {}_{\mathbb{Z}}\mathfrak{M}$)，施以平凡的 G-作用(即取 $\sigma: G \to \mathrm{Aut}A$ 为平凡的同态：$\sigma(G) = I_{\mathrm{Aut}A}$)注意投射 $\mathbb{Z}$-模即自由 $\mathbb{Z}$-模(自由 Abel 群)即得：

命题 12.7 (群的上同调泛系数定理)　设 G 为群，A 为 Abel 群，$A \in {}_{\mathbb{Z}G}\mathfrak{M}$ 按平凡的 G-作用定义，则有可裂的短正合列

$$0 \to \mathrm{Ext}_{\mathbb{Z}}^1(H_{n-1}(G, \mathbb{Z}), A)$$
$$\to H^n(G, A) \to \mathrm{Hom}_{\mathbb{Z}}(H_n(G, \mathbb{Z}), A) \to 0, \ \forall n$$

因此，$H^2(G, A) = 0, \forall A \in {}_{\mathbb{Z}G}\mathfrak{M} \Leftrightarrow G^{ab} \in \mathrm{Free}_{\mathbb{Z}}\mathfrak{M}$ 且 $H_2(G, \mathbb{Z}) = 0$。

可以证明：以 A 为核的 G 之中心扩张(按交换图定义的)同构类，按 Bear 和($\forall (E_1, \varphi_1), (E_2, \varphi_2) \in c.e(G), E = E_1 \times_G E_2 = \{(e_1, e_2) \in E_1 \times E_2 \mid \varphi_1(e_1) = \varphi_2(e_2)\}$ 称为 (E_1, φ_1) 与 (E_2, φ_2) 的 Bear 和)成一与 $H^2(G, A)$ 同构的 Abel 群。平凡的中心扩张对应其单位元(零元)。因此，以 A 为核的 G 的中心扩张都平凡(可裂)$\Leftrightarrow H^2(G, A) = 0$(对乘法群 $=1$)。注意，当 $c.e(G)$ 都平凡时，$\forall A \in {}_{\mathbb{Z}}G$ 都可作为 G 的某一中心扩张的核，于是，G 无非平凡的中心扩张 $\Leftrightarrow H^2(G, A) = 0, \forall A \in {}_{\mathbb{Z}}G$。再由命题 11.1(2)，命题 12.2(2)及命题 12.7，即得如下的有趣结果。

推论 12.1　设 $(E, \varphi) \in c.e(G)$，则

$$(E,\varphi)\in \mathrm{u.c.e}(G) \Leftrightarrow \mathrm{H}_1(E,\mathbb{Z}) \simeq \mathrm{H}_2(E,\mathbb{Z})$$
$$= 0(\text{对乘法群记为“}=1\text{”})$$

由此，我们又有如下结果：$\forall R\in \mathfrak{R}\mathrm{ing}$，$\mathrm{H}_2(\mathrm{St}(R),\mathbb{Z})\simeq \mathrm{H}_1(\mathrm{St}(R),\mathbb{Z})=1$。

§13 K_i 群($i=0,1,2$)关于正向极限的连续性

本节中不要求读者通晓正向极限的理论。先回顾一下偏序集的概念，以方便读者。

定义 13.1 设 S 为一集合且对二元关系 $\leqslant$ 满足：

(O_1) $\forall x\in S, x\leqslant x$（自反性）；

(O_2) $\forall x,y,z\in S, x\leqslant y$ 且 $y\leqslant z$ 时，$x\leqslant z$（可传性）；

(O_3) $\forall x,y\in S, x\leqslant y$ 且 $y\leqslant x$ 时，$x=y$（反对称性），

则称 S 为**偏序集**(poset, partially ordered set)，或拟序集(quasi-ordered set)。只要求满足(O_1)，(O_2)时称 S 为**预序集**(preordered set)。若偏序集 S 又满足

(O_4) $\forall x,y\in S, x\leqslant y$ 或 $y\leqslant x$（可比性），

则称 S 为**全序集**(totally ordered set)，或说 S 有**线性序**。若偏序集 S 又满足

(O_5) $\forall x,y\in S$，必有 $z\in S$ 使 $x\leqslant z$ 且 $y\leqslant z$（有界性），

则称 S 为**正向集**(directed set, direct set)。

例 1 全序集都是正向集（注意(O_4)$\Rightarrow$(O_5)）。

良序集（任一非空子集都有最小元的偏序集）关于其反序（$x\leqslant y$ 变成 $y\leqslant^{-1} x$）为正向集。

格（任二元素都有最小上界与最大下界的偏序集）都是正向集。

例 2 集合 S 子集的集合对包含关系成偏序集，也是正向集。

定义 13.2 设 Λ 为偏序集，$\mathscr{C}$ 为一个范畴，记

$\mathscr{C}_\Lambda=\{M_\lambda\in\mathscr{C}\mid\lambda\in\Lambda, \forall\lambda\leqslant\mu$，有 $\mathscr{C}$ 中态射 $f_{\mu\lambda}:M_\lambda\to M_\mu$ 使 $f_{\lambda\lambda}=1$，
$f_{\gamma\mu}f_{\mu\lambda}=f_{\gamma\lambda}, \forall\lambda\leqslant\mu\leqslant\gamma, \lambda,\mu,\gamma\in\Lambda\}\equiv\{M_\lambda, f_{\mu\lambda}\}\equiv\mathscr{F}$

称为 $\mathscr{C}$ 在 Λ 上的一个**正向系**(direct system)。

注① 这里的 $\mathscr{C}$ 可取 $\mathfrak{G}$，${}_{A}\mathrm{G}$，${}_R\mathfrak{M}$，$\mathfrak{R}$ing，$\mathfrak{S}$et（集范畴），$\overline{\mathrm{T}}$op（拓扑空间范畴）等。有的文献（如[Rotman, 1979]）只要求 Λ 为预序集来定义正向系（不

要求 Λ 满足 O_3，仍可证对 ${}_R\mathfrak{M}$ 等范畴下面的 $\varinjlim$ 存在）。

定义 13.3　设 $\mathscr{F}=\{M_\lambda, f_{\mu\lambda}\}$ 与 $\mathscr{F}'=\{M'_\lambda, f'_{\mu\lambda}\}$ 都是 $\mathscr{C}$ 在 Λ 上的正向系。定义 $\varphi:\mathscr{F}\to\mathscr{F}'$ 为 $\{\varphi_\lambda: M_\lambda\to M'_\lambda \mid f'_{\mu\lambda}\varphi_\lambda=\varphi_\mu f_{\mu\lambda}, \forall\lambda\leqslant\mu\}$，（即

$$\begin{array}{ccc} M_\lambda & \xrightarrow{\varphi_\lambda} & M'_\lambda \\ {\scriptstyle f_{\mu\lambda}}\downarrow & & \downarrow{\scriptstyle f'_{\mu\lambda}} \\ M_\mu & \xrightarrow[\varphi_\mu]{} & M'_\mu \end{array}$$

为交换图）。当 $X\in\mathscr{C}(Ob,\mathscr{C})$ 时，$\varphi:\mathscr{F}\to X$ 指 $\{\varphi_\lambda: M_\lambda\to X \mid \varphi_\lambda=\varphi_\mu f_{\mu\lambda}, \forall\lambda\leqslant\mu\}$（即

$$\begin{array}{ccc} M_\lambda & \xrightarrow{\varphi_\lambda} & X \\ {\scriptstyle f_{\mu\lambda}}\downarrow & \nearrow{\scriptstyle \varphi_\mu} & \\ M_\mu & & \end{array}$$

为交换图）。如果 (X,φ) 具有如下泛性质：任给 $Y\in\mathscr{C}$，$\psi:\mathscr{F}\to Y$，必有惟一的态射 $h:X\to Y$ 使 $\psi_\lambda=h\varphi_\lambda$，$\forall\lambda\in\Lambda$，即

$$\begin{array}{ccc} M_\lambda & \xrightarrow{\varphi_\lambda} & X \\ & {\scriptstyle\psi_\lambda}\searrow & \downarrow{\scriptstyle h}\ \exists 1 \\ & & Y \end{array} \qquad\qquad \begin{array}{ccccc} X & & \xrightarrow[h]{\exists 1} & & Y \\ & \nwarrow{\scriptstyle\varphi_\lambda} & & {\scriptstyle\psi_\lambda}\nearrow & \\ {\scriptstyle\varphi_\mu}\uparrow & & M_\lambda & & \uparrow{\scriptstyle\psi_\mu} \\ & & \downarrow{\scriptstyle f_{\mu\lambda}} & & \\ & & M_\mu & & \end{array}$$

为交换图，则记 $X\equiv M_\infty\equiv\varinjlim M_\lambda$，且称 X 为 $\mathscr{F}$ 的**正向极限**（direct limit）或上极限（colimit），也称**内射极限**（injective limit）。

我们先证明一个常用的结果。

命题 13.1　设 $\mathscr{C}=\mathscr{A}G, {}_R\mathfrak{M}, \mathscr{G}, \mathscr{R}ing, {}_R\mathscr{A}lg$（$R$-代数范畴）。$\mathscr{F}=\{M_\lambda, f_{\mu\lambda}\}_{\lambda\in\Lambda}$ 为 $\mathscr{C}$ 中的正向系，Λ 为正向集，则 $\varinjlim M_\lambda$ 存在且在同构意义下是惟一的。

证　(1) 设 $\mathscr{C}={}_R\mathfrak{M}$（$\mathscr{A}G={}_Z\mathfrak{M}$ 为其特殊情况）。

取 $\{M_\lambda|_{\lambda\in\Lambda}\}$ 的直并（不相交并）

$$X=\dot{\bigcup_{\lambda\in\Lambda}} M_\lambda$$

令 $i_\lambda: M_\lambda\to X$ 为标准单射。在 X 上定义关系"$\equiv$"：$\forall x\in M_\lambda, y\in M_\mu, x\equiv y \Leftrightarrow$ 有 $\nu\in\Lambda$ 使 $\lambda,\mu\leqslant\nu$ 且 $f_{\nu\lambda}(x)=f_{\nu\mu}(y)$。容易看出"$\equiv$"为等价关系。因此

可将 X 分划为等价类的并，记 X 关于"≡"的商集(等价类集)为

$$M_\infty = X/\equiv$$

将 $x\in M_\lambda$ 所在的等价类(有时记为 $\lim x$)记为 $\bar{x}$，$\forall \bar{x},\bar{y}\in M_\infty$，必有 $\alpha,\beta\in\Lambda$ 使 $x\in M_\alpha$，$y\in M_\beta$，但 Λ 为正向集，必有 γ 使 $\alpha,\beta\leqslant\gamma$。因此 $f_{\gamma\alpha}(x)$，$f_{\gamma\beta}(y)\in M_\gamma$ 定义

$$\bar{x}+\bar{y}=\overline{f_{\gamma\alpha}(x)+f_{\gamma\beta}(y)}$$

$\forall r\in R$，定义

$$r\bar{x}=\overline{rx}$$

容易验知 $M_\infty\in{}_R\mathfrak{M}$，且 $\{i_\lambda\}$ 按等价类诱导的 $\{\varphi_\lambda:M_\lambda\to M_\infty\}$ 满足正向极限的各条件，于是 $\varinjlim M_\lambda$ 存在，其同构惟一性用常规证法即可得出。

(2) 设 $C=\mathscr{R}\mathrm{ing}$($\mathscr{G}$，${}_R\mathscr{A}\mathrm{lg}$ 同理可证)，仿(1)进行，只需再仿(1)定义

$$\bar{x}\cdot\bar{y}=\overline{f_{\gamma\alpha}(x)f_{\gamma\beta}(y)}$$

即可。 □

例 3 ${}_R\mathfrak{M}$ 的直和 $\coprod_{\lambda\in\Lambda}M_\lambda$ 为 $\varinjlim M_\lambda$ 的特例(按部分直和与包含关系取正向系。比如

$$\begin{array}{ccc} M_1\subset M_1\oplus M_2 & \subset M_1\oplus M_2\oplus M_3\subset\cdots) \\ \cup & \cup \\ M_2\subset & M_2\oplus M_3 \end{array}$$

但对 $\mathscr{R}\mathrm{ing}$，标准单射 $i_\lambda:R_\lambda\to\bigoplus_{\lambda\in\Lambda}R_\lambda\equiv\coprod_{\lambda\in\Lambda}R_\lambda$ 不保持单位元，因而不是环同态(即，不是 $\mathscr{R}\mathrm{ing}$ 中的态射)，所以 $\coprod_{\lambda\in\Lambda}R_\lambda$ 不是范畴意义下的直和，通常不能构成正向系，比如 $(p,q)=1$ 时 $\{\mathbb{Z}_p,\mathbb{Z}_q\}$ 的正向系不存在，正向极限也不存在。

例 4 $\mathscr{C}$ 中的对象升链(这里设 $\mathscr{C}$ 为具体范畴，即一切对象都是集合)

$$M_1\subset M_2\subset M_3\subset\cdots$$

总存在正向极限且为 $\varinjlim M_\lambda=\bigcup_{\lambda\in\Lambda}M_\lambda$。过去我们多次用过的

$$\mathrm{GL}(R)=\varinjlim\mathrm{GL}_n(R)=\bigcup_{n=1}^{\infty}\mathrm{GL}_n(R)$$

$$\mathrm{E}(R)=\varinjlim\mathrm{E}_n(R)=\bigcup_{n=1}^{\infty}\mathrm{E}_n(R)$$

$$\mathrm{SL}(R)=\varinjlim\mathrm{SL}_n(R)=\bigcup_{n=1}^{\infty}\mathrm{SL}_n(R)\ (R\text{ 为交换环即 }R\in\mathscr{C}\mathrm{Ring}\text{ 时})$$

$$\mathrm{St}(R)=\varinjlim\mathrm{St}_n(R)=\bigcup_{n=1}^{\infty}\mathrm{St}_n(R)$$

等都属此种情况，这就是我们常称它们为"极限"的缘故。

例 5 设 $M\in{}_R\mathfrak{M}$ 的有限生成子模的集合为 $\{M_\lambda\mid\lambda\in\Lambda\}$，按包含关系给

出偏序，则 Λ 为正向集，$\lambda\leqslant\mu$ 时记包含映射（同态）为

$$f_{\mu\lambda}=i_{\mu\lambda}:M_\lambda\to M_\mu$$

则 $\{M_\lambda,f_{\mu\lambda}\}$ 为正向系，且 $\varinjlim M_\lambda=M$。因此，一切 R-模都是其有限生成子模的正向极限。

类似地，用此法可证：任何环 $R\in\mathfrak{Ring}$ 都是 Noether 环的正向极限。事实上，$\mathbb{Z}$ 在 R 中的象 $R_0\equiv\mathbb{Z}1_R$ 为 R 的极小子环。取 $\{R_\lambda\mid\lambda\in\Lambda\}$ 为 R 的在 R_0 上作出的有限生成子环之集合（因而 R_λ 都是 Noether 环），则 $R=\varinjlim R_\lambda$。

注②　可以证明（比如参看[Rotman，1979]）：

（1）$\varinjlim:{}_R\mathfrak{M}\to{}_R\mathfrak{M}$ 为正合函子且与函子 $\otimes$ 可交换；

（2）对偶地（通过反转箭头方向）可定义**反向集，反向系**与**反向极限**（inverse limit）$\varprojlim$（又称为**极限或投射极限**）及其泛性质。为证其存在性（因而为存在惟一性）只需对 $\mathscr{C}$（此为 ${}_R\mathfrak{M}$）中反向系 $\{M_\lambda,f_{\lambda\mu}\}$ 考察 $\prod\limits_{\lambda\in\Lambda}M_\lambda$，取其子模

$$\{(x_\lambda)_{\lambda\in\Lambda}\mid\lambda\leqslant\mu\text{ 时},x_\lambda=f_{\mu\lambda}(x_\mu)\}$$

对偶于命题 13.1 之证，定义等价关系 $\approx$，记其商集为 $M^\approx$。证明它具有 $\varprojlim$ 的泛性质即知

$$M^\approx=\varprojlim M_\lambda$$

存在。对 $\mathfrak{Ring}$ 等范畴，注意标准投射 $P_\alpha:\prod\limits_{\lambda\in\Lambda}M_\lambda\twoheadrightarrow M_\alpha$ 仍为环同态，可类似证明（注意：对 $\mathfrak{Ring}$，虽常将"Π"记为"$\oplus$"，但这是直积而不是直和！）

（3）若 (F,G) 为伴随函子对，则 F 与 $\varinjlim$（不限 Λ 为正向集）可交换，G 与 $\varprojlim$（不限 Λ 为反向集）可交换。比如，$(B\underset{R}{\otimes}-,\mathrm{Hom}_R(B,-))$ 为伴随函子对，因而，$B\underset{R}{\otimes}-$ 与 $\varinjlim$ 可交换 $\mathrm{Hom}_R(B,-)$ 与 $\varprojlim$ 可交换。

由上面的（2）立得命题 13.1 的对偶命题。

命题 13.1°　设 $\mathscr{C}=\mathcal{A}\mathfrak{G},{}_R\mathfrak{M},\mathfrak{G},\mathfrak{Ring},{}_R\mathcal{A}\mathfrak{lg}$，$\mathscr{F}=\{M_\lambda,f_{\mu\lambda}\}_{\lambda\in\Lambda}$ 为 $\mathscr{C}$ 中的反向系且 Λ 为反向集，则 $\varprojlim M_\lambda$ 存在且在同构意义下是惟一的。

例 6　设 p 为素数，$\Lambda=\{1,2,3,\cdots\}$。按标准同态有 $\mathfrak{Ring}$ 中的反向系

$$\mathbb{Z}_p\leftarrow\mathbb{Z}_{p^2}\leftarrow\mathbb{Z}_{p^3}\leftarrow\cdots$$

此时

$$\varprojlim\mathbb{Z}_{p^n}=\mathbb{Z}_{(p)}=\{(a_1,a_2,a_3,\cdots)\mid a_j\in\mathbb{Z}_{p^j},a_j=a_{j-1}\bmod p^{j-1}\}$$

即 ***p*-adic 整数环**，其加、乘运算按分量各自进行加、乘。

更一般地，设 $R\in\mathfrak{Ring}$，$I\triangleleft R$，则

$$R/I \leftarrow R/I^2 \leftarrow R/I^3 \leftarrow \cdots$$

为Ring 中的反向系且

$$\varprojlim R/I^n \equiv R_I$$

称为 R 的 **I-adic 完备化**。对任意的 $M \in {}_R\mathfrak{M}$ 有反向系 $M/IM \leftarrow M/I^2M \leftarrow \cdots$，称

$$\varprojlim M/I^nM$$

为 M 的 **I-adic 完备化**。在赋值论与代数几何及其他一些相关学科中都是有用的工具。

注③ 对 $\mathscr{C} = {}_R\mathfrak{M}$，一般地，$\varprojlim$ 为左正合但非正合函子（见下例）。

例 7 考察行正合交换图

$$\begin{array}{ccccccccc}
 & & \cdots & & \cdots & & \cdots & & \\
 & & \downarrow p & & \downarrow p & & \downarrow p & & \\
0 & \longrightarrow & \mathbb{Z} & \xrightarrow{n} & \mathbb{Z} & \longrightarrow & \mathbb{Z}_n & \longrightarrow & 0 \\
 & & \downarrow p & & \downarrow p & & \downarrow p & & \\
0 & \longrightarrow & \mathbb{Z} & \xrightarrow{n} & \mathbb{Z} & \longrightarrow & \mathbb{Z}_n & \longrightarrow & 0 \\
 & & \downarrow p & & \downarrow p & & \downarrow p & & \\
0 & \longrightarrow & \mathbb{Z} & \xrightarrow{n} & \mathbb{Z} & \longrightarrow & \mathbb{Z}_n & \longrightarrow & 0
\end{array}$$

其中 $(n,p)=1$，$\xrightarrow{x}$ 表示乘 x 所得的 ${}_{\mathbb{Z}}\mathfrak{M} = \mathcal{A}G$ 同态，各列均为反向系。左边两列的反向极限为 0，但右列的箭头都是同构，因此右列的反向极限为 $\mathbb{Z}_n$。于是

$$0 \to 0 \to \mathbb{Z}_n$$

正合。但 $0 \to \mathbb{Z}_n$ 不是满同态，由此知 $\varprojlim$ 不是正合函子。

例 8 设 $R \in \mathcal{C}$Ring，A, B, C 为交换的 R-代数（比如交换环都是 $\mathbb{Z}$-代数）。可以验证：

（1） $\begin{array}{ll} p_1: & A \to A \otimes_R B \\ & x \mapsto x \otimes 1 \end{array}$，$\begin{array}{ll} p_2: & B \to A \otimes_R B \\ & y \mapsto 1 \otimes y \end{array}$ 均为 R-代数同态；

（2） 对任意的 R-代数同态 $f: A \otimes_R B \to C$，$g = fp_1: A \to C$ 与 $h = fp_2: B \to C$ 均为 R-代数同态；

（3） 对任意的 R-代数同态 $g: A \to C$ 与 $h: B \to C$ 必有惟一的 R-代数同态 $f: A \otimes_R B \to C$（即 $f(x \otimes y) = g(x)h(y)$）使下页的图为交换图。

$$\begin{array}{ccc} A\otimes_R B & \xleftarrow{p_2} & B \\ {\scriptstyle p_1}\uparrow & \overset{f}{\searrow}\ \exists 1 & \downarrow{\scriptstyle h} \\ A & \xrightarrow[g]{} & C \end{array}$$

因此,给出 R-代数同态 $f:A\bigotimes\limits_R B\to C$ 相当于给出一对 R-代数同态 $g:A\to C$,$h:B\to C$。由此,知 $A\bigotimes\limits_R B$ 为 A,B 在 $_R\mathcal{A}$lg 中的直和(特殊的正向极限)。

现在证明 K_0 群在正向极限下的连续性。

定理 13.1　设$\{R_\alpha,f_{\beta\alpha}:R_\alpha\to R_\beta,\alpha\leqslant\beta,\alpha,\beta\in\Lambda\}$为$\mathcal{R}$ing 中的正向系,$\Lambda$ 为正向集,则

$$K_0(\varinjlim R_\alpha)\simeq\varinjlim K_0(R_\alpha)$$

证　由 K_0 为共变函子知,K_0 将$\mathcal{R}$ing 中的交换图变为$\mathcal{A}$G 中的交换图且保持恒等态射对应。因此

$$\{K_0(R_\alpha),K_0(f_{\beta\alpha}):K_0(R_\alpha)\to K_0(R_\beta),\alpha\leqslant\beta,\alpha,\beta\in\Lambda\}$$

为$\mathcal{A}$G 中的正向系。由命题 13.1 知必有惟一(同构意义下)的正向极限$\varinjlim K_0(R_\alpha)$。再由正向极限的泛性质知,必有(标准)群同态

$$f:\varinjlim K_0(R_\alpha)\to K_0(\varinjlim R_\alpha)$$

下证 f 为群同构即可。

先证 f 为满同态,为简化记号,记 $R=\varinjlim R_\alpha$,用 K_0 群的幂等阵定义(见§2)。任取 $p^2=p\in\mathrm{Idem}(R)$,则 $p\in R^{\infty\times\infty}$ 且 p 中具有有限个 R 中的非零元。于是由 Λ 为正向集知,必有 $\gamma\in\Lambda$ 使 $p\in\mathrm{Im}(\mathrm{Idem}(R_\gamma)\to\mathrm{Idem}(R))$,但在 $K_0(R)$中,$[p]\in\mathrm{Im}(K_0(R_\gamma)\to K_0(R))$。因此由交换图

$$\begin{array}{ccc} K_0(R_\gamma) & \to & K_0(R) \\ \downarrow\varphi_\gamma & \nearrow f & \\ \varinjlim K_0(R_\alpha) & & \end{array}$$

知$[p]\in\mathrm{Im}(\varinjlim K_0(R_\alpha)\to K_0(R))=\mathrm{Im}f$。而仿定理 1.1 之证可知 $K_0(R)=\{[p]-[q]\mid p,q\in\mathrm{Idem}(R)\}$,因此 f 为满同态。

再证 f 为单同态,任取 $x\in\mathrm{Ker}f$,即 $f(x)=0\in K_0(R)$。仿上面的交换图知必有 $\alpha\in\Lambda$ 使 $x\in K_0(R_\alpha)$且 $x=[p]-[q]$,$p^2=p$,$q^2=q\in\mathrm{Idem}(R_\alpha)$,于是在 $K_0(R)$中 $f([p])=f([q])$。由§2 知必有 $A\in GL(R)$使 $ApA^{-1}=q$,因此必有 $\gamma\in\Lambda,\gamma\geqslant\alpha$ 使 $f_{\gamma\alpha}:[p]-[q]\mapsto 0\in K_0(R_\gamma)$。于是由交换图

$$\begin{array}{ccc} K_0(R_\gamma) & \xleftarrow{f_{\gamma\alpha}} & K_0(R_\alpha) \\ \downarrow \varphi_\gamma & \swarrow \varphi_\alpha & \\ \varinjlim K_0(R_\alpha) & & \end{array}$$

知 $x=0\in\varinjlim K_0(R_\alpha)$，即 f 为单同态。 □

下面举一例子说明由上述定理可给出一个单环 R 使 $K_0(R)\notin \text{f. g. }_{\mathbb{Z}}\mathfrak{M}=\text{f. g. }\mathcal{A}G$。事实上，判定 K_0 群（K_i 群）的有限生成性是代数 K-理论中的一个重要问题。因为知道了 K_i 群的有限生成系有助于用有限生成 Abel 群的基本定理判断 K_i 群的结构。

例 9 设 F 为域，

$$f_n: F^{2^n\times 2^n}\to F^{2^{n+1}\times 2^{n+1}}$$

$$A\mapsto\begin{pmatrix} A & \\ & A\end{pmatrix}$$

在 f_n 作用下，$\forall\, p^2=p\in F^{2^n\times 2^n}$，$[p]\mapsto[p\oplus p]=2[p]$。

记 $R=\varinjlim(F^{2^n\times 2^n}=R_n, f_n)$，由

$$K_0(F^{2^n\times 2^n})\simeq K_0(F)\simeq\mathbb{Z}\simeq K_0(F^{2^{n+1}\times 2^{n+1}})$$

知

$$K_0(R)=\varinjlim(\mathbb{Z}\xrightarrow{2}\mathbb{Z}\xrightarrow{2}\mathbb{Z}\xrightarrow{2}\cdots)\simeq\mathbb{Z}[\frac{1}{2}]$$

注意 $F^{2^n\times 2^n}$ 为单环，R 也必为单环。事实上，$\forall\, x\in R$，必有 $m\geqslant 1$ 使 $x\in F^{2^m\times 2^m}$，但 $F^{2^m\times 2^m}$ 为单环，于是 x 生成的理想 $(x)=0$ 或 $(x)=F^{2^m\times 2^m}$。由此知，在 R 中 x 生成的理想 $(x)=0$ 或 $(x)=R$。因此 R 为单环，而显然 $\mathbb{Z}[\frac{1}{2}]\notin \text{f. g}_{\mathbb{Z}}\mathfrak{M}$。

下面给出 K_1 群与 K_2 群在正向极限下的连续性，它们的证明都可仿定理 13.1 之证给出。

定理 13.2 设 $\{R_\alpha, f_{\beta\alpha}: R_\alpha\to R_\beta, \alpha\leqslant\beta, \alpha,\beta\in\Lambda\}$ 为 Ring 中的正向系，Λ 为正向集，则

$$K_1(\varinjlim R_\alpha)\simeq\varinjlim K_1(R_\alpha)$$

定理 13.3 设 $\{R_\alpha, f_{\beta\alpha}: R_\alpha\to R_\beta, \alpha\leqslant\beta, \alpha,\beta\in\Lambda\}$ 为 Ring 中的正向系，Λ 为正向集，则

$$K_2(\varinjlim R_\alpha)\simeq\varinjlim K_2(R_\alpha)$$

事实上可证：群的同调函子 H_i 与 $\varinjlim$ 可交换，即，对 G 中的正向系 $\{G_\alpha, f_{\beta\alpha}: G_\alpha\to G_\beta, \alpha\leqslant\beta, \alpha,\beta\in\Lambda\}$，

$$H_j(\varinjlim G_\alpha, M) \simeq \varinjlim H_j(G_\alpha, M), \quad \forall M \in {}_{ZG}\mathfrak{M}$$

（这里的 $G=\varinjlim G_\alpha$）。取 $M=Z, G_\alpha=GL(R_\alpha)$，由上节定理 12.1 即得定理 13.2。取 $M=Z, G_\alpha=E(R_\alpha)$，由定理 12.2 即得定理 13.3。

注④　K_i 群（$i=0,1,2$）与 $\varprojlim$ 无类似于定理 13.1，定理 13.2，定理 13.3 的结果，这由以后将介绍的关于拉回图的 K_i 群正合列即知。

下面就 ${}_R\mathfrak{M}$（对此范畴只要求 Λ 为预序集即可证 $\varinjlim$，$\varprojlim$ 存在，见[Rotman，1979]。容易看出（由定理 13.1 之证），下面（例 11）的拉回图对 Ring 也成立），说明**推出**（pushout）图给出正向系，因此推出图为正向极限的特例。而**拉回**（pullback）图为给出反向系，因而拉回图为反向极限的特例。

例 10

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ g\downarrow & \ulcorner\bullet & \\ C & & \end{array} \tag{1}$$

为 ${}_R\mathfrak{M}$ 中的正向系。存在惟一（同构意义下）的 D，与 j_1, j_2 使

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ g\downarrow & \ulcorner\bullet & \downarrow j_1 \\ C & \xrightarrow{j_2} & D \end{array} \tag{1$'$}$$

为交换图，且具有泛性质：$\forall j_1' : B\to D', j_2' : C\to D'$，若 $j_1' f = j_2' g$，则必有惟一的 $h: D\to D'$ 使 $hj_i = j_i', i=1,2$，称(1)′为(1)的**推出(图)**，也称为纤维和（上积）。事实上 $D=\varinjlim(1)$。

如果 $g=0$，则 $\mathrm{Coker} f\simeq D$。因此 Coker 事实上是推出的特例，而推出又是正向极限的特例。

例 11

$$\begin{array}{ccc} & & B \\ & \bullet\lrcorner & \downarrow f \\ C & \xrightarrow{g} & A \end{array} \tag{2}$$

为 ${}_R\mathfrak{M}$ 或 Ring 中的反向系。因此存在惟一的 D 与 j_1, j_2 使

$$\begin{array}{ccc} D & \xrightarrow{j_1} & B \\ j_2\downarrow & \bullet\lrcorner & \downarrow f \\ C & \xrightarrow{g} & A \end{array} \tag{2$'$}$$

为交换图且具有泛性质：$\forall j_1' : D'\to B, j_2' : D'\to C$，必有惟一的 $h: D'\to D$ 使

$j_i h = j_i'$，$i=1,2$，称(2)′为(2)的**拉回(图)**。事实上 $D = \varprojlim(2)$。

在 $g=0$ 时，$\mathrm{Ker} f \simeq D$。因此 Ker 事实上为拉回的特例，而拉回又是反向极限的特例。

拉回的应用更广，也称为**纤维积**(fiber product)(B，C 在 A 上的纤维积)或 **Descartes 方(图)**。

对$\mathfrak{R}$ing(环范畴)(${}_R\mathfrak{M}$ 仿此)不但可证：任意的环同态 $f_j: R_j \to S$，$j=1,2$ 的拉回(纤维积，Descartes 方)存在(因而在同构意义下惟一)。而且可具体构作如下：

在 $R_1 \oplus R_2$ 中取

$$T = \{(r_1, r_2) \in R_1 \oplus R_2 \mid f_1(r_1) = f_2(r_2)\}$$

显然 T 为 $R_1 \oplus R_2$ 的子环。令

$$g_j = p_j \mid_T,$$

其中 $p_j: R_1 \oplus R_2 \to R_j$ 为标准环同态($p_j(x_1, x_2) = x_j$，$j=1,2$)，则有拉回图

$$\begin{array}{ccc} T & \xrightarrow{g_1} & R_1 \\ {\scriptstyle g_2}\downarrow & \lrcorner & \downarrow{\scriptstyle f_1} \\ R_2 & \xrightarrow[f_2]{} & S \end{array}$$

即环 T 为 R_1，R_2 在 S 上的(关于 f_1，f_2)的纤维积。显然 f_2 单(满) $\Leftrightarrow$ g_1 单(满)，f_1 单(满) $\Leftrightarrow$ g_2 单(满)，这是后文常用的 Descartes 方图。

例 12　$\forall R \in \mathfrak{R}$ing，$I_j \lhd R$，$j=1,2$，取标准环同态

$$f_j: R/I_j \to R/(I_1 + I_2) = S$$

$$g_j: T = R/I_1 \cap I_2 \to R/I_j$$

则有拉回图

$$\begin{array}{ccc} R/I_1 \cap I_2 & \xrightarrow{g_1} & R/I_1 \\ {\scriptstyle g_2}\downarrow & \lrcorner & \downarrow{\scriptstyle f_1} \\ R/I_2 & \xrightarrow[f_2]{} & R/(I_1 + I_2) \end{array}$$

此例可看成是下述($n=2$ 时)**中国剩余定理**(CRT，Chinese Remainder Theorem)的推广：

设 $R \in \mathfrak{R}$ing，$I_j \lhd R$，$j=1,2,\cdots,n$。且 $I_i + I_j = R$，$\forall i \neq j$，则有标准环(满)同态

$$\varphi: R \twoheadrightarrow R/I_1 \oplus \cdots \oplus R/I_n$$

$$r \mapsto (r + I_1, \cdots, r + I_n)$$

且 $\mathrm{Ker}\varphi = \bigcap_{j=1}^{n} I_j$，因此 $R/\bigcap_{j=1}^{n} I_j \simeq R/I_1 \oplus \cdots \oplus R/I_n$。

当 $R=\mathbb{Z}, I_j=(m_j)\lhd\mathbb{Z}, (m_i,m_j)=1, \forall i\neq j$ 时，对任意的 $b_j\in\mathbb{Z}, j=1, 2,\cdots,n$ 同余方程组

$$x\equiv b_j(\mathrm{mod}\ m_j),\qquad j=1,2,\cdots,n$$

必有解。且在 mod m 意义下惟一，其中 $m=m_1\cdots m_n, (m)=\bigcap_{j=1}^{n}(m_j)$。

注⑤　CRT 有更广的形式(证明可见[Hungerford, 1980])，即在 $\mathfrak{R}$ng 中的 CRT：设 $I_j\lhd R, R\in\mathfrak{R}$ng(不要求有单位元的环范畴)，$R^2+I_j=R, \forall j$ ($R\in\mathfrak{R}$ing 时，此条件当然)，且 $I_i+I_j=R, \forall i\neq j$，则对 R 中任意的 $b_1, b_2, \cdots, b_n$，必有 $b\in R$ 使

$$b\equiv b_j(\mathrm{mod} I_j),\qquad j=1,2,\cdots,n$$

且 $b(\mathrm{mod}\ I_1\cap\cdots\cap I_n)$ 惟一，即

$$R/I_1\cap\cdots\cap I_n\simeq R/I_1\oplus\cdots\oplus R/I_n$$

由此可知，当 $R\in\mathfrak{R}$ing 时，

$$\mathrm{K}_i(R/I_1\cap\cdots\cap I_n)\simeq\mathrm{K}_i(R/I_1)$$
$$\oplus\cdots\oplus\mathrm{K}_i(R/I_n),\qquad i=0,1,2$$

特别地，(a) 当 $I_j\in\mathrm{Max}R, j=1,2,\cdots,n, R\in\mathfrak{C}$Ring 时

$$\mathrm{K}_0(R/I_1\cap\cdots\cap I_n)=\mathrm{K}_0(R/I_1\cdots I_n)\simeq\mathbb{Z}^n$$
$$\mathrm{K}_1(R/I_1\cap\cdots\cap I_n)=\mathrm{K}_1(R/I_1\cdots I_n)$$
$$\simeq(R/I_1\oplus\cdots\oplus R/I_n)^{\cdot}\simeq(R/I_1\cdots I_n)^{\cdot}$$

(b) 当 R 为代数数域 F 中的代数整元环 O_F 时，由引理 7.4 已知 O_F/M 为有限域。这里 $M\in\mathrm{Max}\ O_F$。以后将证：有限域的 K_2 群都是平凡的。因此有：设 $R=O_F, I_j\in\mathrm{Max}R, j=1,2$，则

$$\mathrm{K}_2(O_F/I_1\cap\cdots\cap I_n)=1。$$

§14　K_0 群与拓扑 K^0 群——代数 K-理论与拓扑 K-理论的一个联系

二十世纪三十年代在微分流形的同胚不变量的研究中出现了纤维丛的思想，它是拓扑积的自然推广。它的第一个一般性的定义是 H. Whitney 于 1937 年给出的，H. Hopf 与 E. Stiefel 也作出早期的奠基性工作。四十年代陈省身(S. S. Chen)等发展了这种理论，在示性数理论中作出了重要的工作。现在，纤维丛理论不但在几何学、拓扑学中已占有重要地位，而且在分

析学及物理学中的规范场理论中也是有用的工具之一，五十年代后，特别是六十年代，纤维丛的重要特例一向量丛更引起代数学家们的关注与研究（参看本书引言部分）。

定义 14.1 设 E，B 为拓扑空间，p：E→B 为连续（满）映射，对 $\forall b \in B$，称 $p^{-1}(b)$ 为 p 在 b 点的纤维（fibre），且称（E，p，B）为 B 上的一个丛（bundle）。若 p：E→B 又满足下述两条件：

（1）$\forall b \in B, p^{-1}(b) \in {}_F\mathfrak{M}$（域或除环 F 上的模（向量空间），事实上 $p^{-1}(b) \in \text{f. g. Free}_F\mathfrak{M}$；

（2）（局部平凡性）$\forall b \in B$，都有开邻域 U_b 与 $n = n(b)$ 使有同胚映射

$$\psi: U_b \times F^n \simeq p^{-1}(U_b)$$

且 ψ（限制在 $b \times F^n$ 上）也是 F-同态，则称（E，p，B）为 B 上的一个**向量丛**（vector bundle）也称为**局部有限向量丛**（locally finite vector bundle），E 称为此丛的**全空间**，B 称为此丛的**基空间**（底空间），p 称为此丛的**丛投射**，常记（E，p，B）$\in \mathcal{V}ec(B)$ 或 E $\in \mathcal{V}ec(B)$。若有连续映射 s：B→E 使 $ps = I_B$，则称 s 为此丛的**截面**（section），记为 $s \in \Gamma(\text{E})$，$\Gamma(\text{E})$ 又称**向量场**（vector field）。

设（E，p，B），（E′，p'，B）$\in \mathcal{V}ec(B)$ 可定义丛运算（称为**纤维积**或 **Whitney 和**）：

$$\text{E} \oplus \text{E}' = \{(e, e') \in \text{E} \times \text{E}' \mid p(e) = p'(e')\} \xrightarrow[q]{} B, \; q(e, e') = p(e) = p'(e')$$

事实上是

$$\begin{array}{ccc} & & E' \\ & & \downarrow p' \text{的拉回图} \\ E & \xrightarrow[p]{} & B \end{array}$$

$$\begin{array}{ccc} E \oplus E' & \xrightarrow{p_2} & E' \\ p_1 \downarrow & & \downarrow p' \\ E & \xrightarrow[p]{} & B \end{array} \qquad p_1, p_2 \text{ 为标准投射}$$

还可定义（E，p，B）与（E′，p'，B）间的丛同态为使下图为交换图的连续映射 φ：E→E′，

$$\begin{array}{ccc} & & E' \\ & \overset{\varphi}{\nearrow} & \downarrow p' \\ E & \xrightarrow[p]{} & B \end{array}$$

由此可记$[E]$为(E,p,B)所在的同构类(与$\oplus$相容)。B 上全体向量丛的同构类集合仍以$\mathcal{V}ec(B)$记之。于是$\mathcal{V}ec(B)$为 Abel 半群,其群的完备化(见§1)称为$\mathcal{V}ec(B)$或 B 的 Grothendieck 群(K-群),在拓扑上常记为 $K_F^0(B)$, $K^0(B)$或 $K(B)$。当 $F=\mathbb{R}$ 时也记为 $KO(B)$("O"表示"正交(orthogonal)"),$F=\mathbb{C}$ 时也记为 $KU(B)$("U"表"酉(unitary)")。

定义 14.1 中的 $n=n(b)$给出一个连续秩函数

$$\begin{aligned}\mathrm{rank}_E : B &\to \mathbb{N}\\ b &\mapsto \dim p^{-1}(b) \equiv n = n(b)\end{aligned}$$

当 B 连通时,rank_E 为常值函数,此时约化 K-群定义为

$$\begin{aligned}\widetilde{K}_F^0(B) = \mathrm{Ker}(\mathrm{rank}_E : K_F^0(B) &\to \mathbb{Z})\\ [E] &\mapsto n\end{aligned}$$

因此对连通空间,约化 K 群成为可代表 K 群的研究对象。

当 B 为紧致 Hausdorff 空间(定义见后)时,记 $C(B)$为 B 上实连续函数环,则有同胚 $B\simeq \mathrm{Max}B$,可用§4 中局部化方法与后面的 Swan 定理将 $\widetilde{K}_F^0$ 定义开拓到非连通的紧致 Hausdorff 空间。

注①　对(E,p,B),$(E',p',B)\in\mathcal{V}ec(B)$,通过对每一点 $b\in B$ 的纤维 $p^{-1}(b)$与 $p'^{-1}(b)$(作为${}_F\mathfrak{M}$)的张量积 $p^{-1}(b)\otimes p'^{-1}(b)$可定义 $E\otimes E'$(可验证与同构相容)使$\mathcal{V}ec(B)$为半环(与环相比,不要求满足环中对"+"为 Abel 群只要求为 Abel(幺)半群)。由此知,作为半环的环完备化,$K^0(B)$为一个交换环(参看§1,注①)。

对任意的 $X,Y\in\mathrm{Top}$(拓扑空间范畴)与连续映射 $f:X\to Y$,设 F 为域, $C(X)$表示一切连续函数 $g:X\to F$ 所成的交换环(运算$+$,$\times$按函数$+$,$\times$的逐点定义法定义)。由交换图

$$\begin{array}{ccc} X & \xrightarrow{f} & Y\\ & g^*=gf \searrow \quad \swarrow g & \\ & F & \end{array}$$

定义 $C:C(Y)\to C(X)$使 $C(g)=g^*=gf$。可验知

$$C:\mathrm{Top}\to \mathbb{C}\mathrm{Ring}$$

为一个反变函子。

任给$(E,p,Y)\in\mathcal{V}ec(Y)$与连续映射 $f:X\to Y$,注意对 Top,$\varprojlim$肯定存在。用拉回图(更广义的纤维积)

$$\begin{array}{ccc} f^*(Y) & \xrightarrow{p_2} & E \\ p_1 \downarrow & & \downarrow p \\ X & \xrightarrow{f} & Y \end{array}$$

其中

$$f^*(Y) = X \times_Y \mathrm{E} = \{(x,e) \in X \times \mathrm{E} \mid f(x) = p(e)\}$$

给出$(f^*(Y),p_1,X)\in$ Vec(X)。于是，我们又有一个反变函子 V:Top→SG(半群范畴),SRing(半环范畴)。因此有关于函子的交换图(其中 G 表示群完备化(共变)函子,R 表示环完备化(共变)函子):

Top

(反变)V ↓ ↘ K^0(反变)

SG (SRing) $\xrightarrow{\text{G (R)}}$ AG (CRing)

这里,自然要问:对什么样的拓扑空间(Top 的什么样的子范畴),下图是(同构意义下的)交换图。

Top ⟶ CRing

↘ C(反变) ↓ K^0

K^0(反变) ↘

CRing

1955 年,J. P. Serre 在他的著名论文 FAC([Serre,1955])中证明了:仿射(代数)簇上向量丛与此仿射(代数)簇坐标环上有限生成投射模是一一对应的。事实上,他证明出:取 Top 的子范畴—仿射(代数)簇范畴,则上图是交换的。1962 年 R. Swan 在[Swan,1962]中更进一步地证明了:紧致 Hausdorff 空间 X 上的向量丛范畴等价于 $C(X)$ 上有限生成投射模范畴,因此 $K^0(X)\simeq K_0(C(X))$,即对Top 的更大的子范畴 CH(紧致 Hausdorff 空间范畴),上图是交换的。这里的紧致(compact)是指具有有限覆盖性质。而 X 为 Hausdorff 空间是指:$\forall\, p,q\in X$,必有 p,q 的开邻域U_p,U_q 使 $U_p\cap U_q=\varnothing$(可分离性)。1984 年 K. R. Goodearl 在[Goodearl,1984]又将 Swan 的结果(代数与拓扑间的一个著名桥梁通道)开拓到仿紧(paracompact) Hausdorff 空间上的有限型向量丛。仿紧是指局部有限开覆盖性质,即任给 X 的一个开覆盖,对任意的 $x\in X$,必有 x 的开邻域 U_x 使与此开覆盖的一个加细(refinement,这里 X 的子集族 $\mathscr{B}$ 为子集族 $\mathscr{A}$ 的加细是指:$\forall\, B\in\mathscr{B}$ 必有 $A\in\mathscr{A}$ 使 $B\subseteq A$)只有有限个相交,这是由 1944 年 J. Dieudonné 提出的

一个重要概念,有限型向量丛定义见后。1986 年,L. N. Vaserstein 在[Vaserstein,1986]又将 Goodearl 的结果大大地推进到一般的拓扑空间上的有限型向量丛。本节中将介绍 Vaserstein 结果与证法。

先从具体例子入手,介绍有关概念与基本性的结果。

将 $I\equiv[0,1]$(闭区间)通过粘合 0,1 得 S^1(一维球面,即圆)。

对 $[0,1]\times\mathbb{R}$ 粘合 $(0,x)$ 与 $(1,x)$, $\forall x\in\mathbb{R}$,得 $S^1\times\mathbb{R}$(圆柱面),即 S^1 上的 1 维平凡向量丛($X\times F^n$ 称为 X 上关于域 F 的 n 维平凡向量丛)。若对 $[0,1]\times\mathbb{R}$ 粘合 $(0,x)$ 与 $(1,-x)$, $\forall x\in\mathbb{R}$,则得一个 Möbius 带(单侧曲面)。这是 S^1 上的又一个 1 维向量丛, $\forall x\in[0,1]$,纤维 $p^{-1}(x)=\{x\}\times\mathbb{R}\simeq\mathbb{R}$。

记

$$R\equiv C(S^1)=\{f\in C[0,1]\mid f(0)=f(1)\}$$

则 R 为 $C[0,1]$($[0,1]$上的连续函数环)的子环。记 $E=(E,p,S^1)$ 为圆柱面(S^1 上的平凡向量丛)或 Möbius 带,其截面集记为 $\Gamma(E)=\{s:S^1\to E\mid ps=I_{S^1}\}$。对 $\Gamma(E)$ 逐点式(同函数)定义加法与纯量乘法(R 乘):

$$(s+t)(x)=s(x)+t(x),$$

$$(rs)(x)=r(x)s(x),\quad \forall s,t\in\Gamma(E),r\in R\equiv C(S^1),x\in S^1$$

则使 $\Gamma(E)\in{}_R\mathfrak{M}$。

(1) 对圆柱面 $S^1\times\mathbb{R}$,截面为连续映射

$$s:S^1\to S^1\times\mathbb{R}$$
$$x\mapsto(x',x'')$$

由 $ps=I_{S^1}$ 知 $x'=x$。因此截面 s 由映射

$$S^1\to\mathbb{R}$$
$$x\mapsto x''$$

惟一确定。但 $(x,x'')\in S^1\times\mathbb{R}\underset{1-1}{\leftrightarrow}R=C(S^1)$。因此

$$\Gamma(S^1\times\mathbb{R})\simeq R\in f.g.\,\mathrm{Free}_R\mathfrak{M}\text{(秩为 1)}$$

(2) 对 Möbius 带 (E,p,S^1),仿上知,作为 $C[0,1]$的子环,

$$\Gamma(E)=\{s\in C[0,1]\mid s(0)=-s(1)\}$$

由连续函数性质知必有 $x\in[0,1]$使 $s(x)=0$。因此 E 的任何截面 S 都在 $[0,1]$上有零点。下面来证:

对 Möbius 带 (E,p,S^1), $\Gamma(E)$ 为秩等于 1 的有限生成投射 R-模,但非自由 R-模(因此 $R\notin\mathrm{PF}$)。

事实上,取第二个 Möbius 带 (E_1,p_1,S^1),则

$$E\oplus E_1=\{(e,e_1)\in E\times E_1\mid p(e)=p_1(e_1)\}$$

是粘贴$[0,1]\times\mathbb{R}^2$的$(0,y,z)$与$(1,-y,-z)$而得，$\forall (y,z)\in\mathbb{R}^2$。E，$E_1$可视作此丛分别取$z=0$，$y=0$时的嵌入。由

$$\det\begin{vmatrix} \cos\frac{x}{\pi} & \sin\frac{x}{\pi} \\ -\sin\frac{x}{\pi} & \cos\frac{x}{\pi}\end{vmatrix} = 1 \neq 0$$

知$(\cos\frac{x}{\pi},\sin\frac{x}{\pi})$，$(-\sin\frac{x}{\pi},\cos\frac{x}{\pi})$为$\mathbb{R}^2$之基。定义截面

$$s_1 : x \mapsto (x, \cos\frac{x}{\pi}, \sin\frac{x}{\pi})$$

$$s_2 : x \mapsto (x, -\sin\frac{x}{\pi}, \cos\frac{x}{\pi})$$

则s_1,s_2为$\Gamma(E\oplus E_1)\in f.g.\,\mathrm{Free}_R\mathfrak{M}$之基。于是

$$\Gamma(E)\oplus\Gamma(E_1)\simeq\Gamma(E\oplus E_1)\simeq R^2$$

由此知$\mathrm{rank}\Gamma(E)=1$且$\Gamma(E)\in f.g.\,P_R\mathfrak{M}$。

反设$\Gamma(E)\in\mathrm{Free}_R\mathfrak{M}$，由$R\in\mathrm{CRing}\subset\mathrm{IBN}$知$\Gamma(E)\simeq R$。但由上知E的截面都有零点，于是$\forall s\in\Gamma(E)$，$r\in R$，$rs$在$[0,1]$上也有零点。但对$s:S^1\to 1$（即$s(S^1)=1$），$s\in R$，$s$无零点。于是$\Gamma(E)$不能有基，这与$\Gamma(E)\simeq R$矛盾。于是$\Gamma(E)\notin\mathrm{Free}_R\mathfrak{M}$。

事实上，可不用后面的结果而直接证出：S^1上的实向量丛E的截面集$\Gamma(E)\in f.g.\,P_R\mathfrak{M}$，且$\forall M\in f.g.\,P_R\mathfrak{M}$，都有$S^1$上的实向量丛E使$\Gamma(E)\simeq M$（作为$R$-模），因此$K^0_{\mathbb{R}}(S^1)\simeq K_0(R)$（是Abel群同构，也是环同构）。

对于S^1上的n维实向量丛（纤维都同构于$\mathbb{R}^n$的实向量丛）$\xi=E\xrightarrow{p}S^1$，可以认为$E=[0,1]\times\mathbb{R}^n$且$(0,x)=(1,Ax)$，$A\in GL_n(\mathbb{R})$，可证：

$\det A>0$时，$\xi=\overset{n}{\times}$圆柱面（n个圆柱面之积），$\Gamma(E)\simeq\overset{n}{\underset{j}{\bigoplus}}C(S^1)=R^n$。

$\det A<0$时$\xi=$Mӧbius带$\times(\overset{n-1}{\underset{1}{\times}}$圆柱面$)$，$\Gamma(E)\simeq M\oplus R^{n-1}$，其中$M$为Mӧbius带的截面集。

可以算出（与§3作比较）：

$$K_0(C(S^1))\simeq\mathbb{Z}\oplus\mathbb{Z}_2=\langle[C(S^1)],[C(S^1)]-[M]\rangle$$

为介绍Vaserstein的结果，先给出

定义 14.2 设$X\in\mathrm{Top}$，$\xi=(E,p,X)\in\mathrm{Vec}(X)$。若有$X$到$F=\mathbb{R},\mathbb{C},\mathbb{H}$（实四元数体）的非负连续函数有限集$S=\{f_1,f_2,\cdots,f_n\}$使

(1) $\sum_{j=1}^{n} f_j = 1$；

(2) ξ 在 $\{x\in X\mid f_j(x)\neq 0\}$($f_j$ 的支撑(集)(support))$\subset X$ 上的限制为平凡丛,$j=1,2,\cdots,n$,
则称 ξ 为 X 上的**有限型**(finite type)**向量丛**,记为 $\xi\in$ f. t. $\mathcal{V}$ec(X)。

引进这个定义的目的是排除不能从 f. g. $P_{C(X)}\mathfrak{M}$ 对应到的无限维向量丛。注意,当 X 为紧致 Hausdorff 空间时,X 上的(局部有限)向量丛(见定义 14.1)都是有限型的。因此后面的定理 14.1 概括了 Swan 的结果。

对正规空间(normal space)X,即 X 的不相交闭集都有不相交的开邻域(等价于 Урысон(Urysohn)定理成立:对 X 中任意不相交闭集 A,B,必有连续函数 $f:X\to[0,1]$ 使 $f(A)=0,f(B)=1$,紧致 Hausdorff 空间与度量空间都是正规空间),可证上述定义等价于:有 X 的有限开覆盖 T 使 $\forall U\in T$,限制在 U 上的向量丛都是平凡的。

定理 14.1(Vaserstein,1986)　设 X 为拓扑空间,$F=\mathbb{R},\mathbb{C}$ 或 $\mathbb{H}$(实四元数体)则 f. t. $\mathcal{V}$ec(X)与 f. g. $P_{C(X)}\mathfrak{M}$ 是等价的范畴,因此

$$\text{f. t. } K_F^0(X)\simeq K_0(C(X))$$

其中 $C(X)$为 X 到 F 的连续函数环,上述同构是 Abel 群同构,也是(交换)环同构,f. t. $K_F^0(X)$表示 f. t. $\mathcal{V}$ec(X)仿前定义的 K_0 群。

为证定理 14.1,先在定理 14.1 的条件下证几条引理。

注意与 $F=\mathbb{C}$ 一样对 $F=\mathbb{H}$ 也可定义 Hermite 矩阵:若 $A=A^*\equiv\bar{A}^T\in\mathbb{H}^{n\times n}$,则称 A 为 $\mathbb{H}$ 上的 n 阶 Hermite 矩阵,其中 $\bar{A}=(\bar{a}_{ij})$,T 表转置。而 $\alpha=a+bi+cj+dk\in\mathbb{H}$ 时,其共轭为 $\bar{\alpha}=a-bi-cj-dk$,仿此,当 $F=\mathbb{C}$ 或 $\mathbb{H}$ 时,对 $\forall g\in C(X)$可定义其共轭为 $\bar{g}$,使 $\bar{g}(x)=\overline{g(x)}$,于是又可定义 $C(X)$上的 Hermite 矩阵。

引理 14.1　设 $P\in$ f. g. ${}_{C(X)}\mathfrak{M}$,则必有 $n\in\mathbb{N}$ 与(关于 F 的)n 阶幂等的 Hermite 矩阵 $e=e^2=e^*\in C(X)^{n\times n}$使有${}_{C(X)}\mathfrak{M}$ 同构 $P\simeq\mathrm{col}(e)$(e 的列空间,即 $e(C(X)^{n\times 1})$)。

证　由设可令 P 为 $C(X)^n$ 的直和项,即有 $Q\in{}_{C(X)}\mathfrak{M}$ 使得 $P\oplus Q=C(X)^n$。记 $p_1:P\oplus Q\to P$ 为第一直和项的标准投射,在 $C(X)^n$ 某一基下对应的矩阵为 a,则 $a=a^2\in C(X)^{n\times n}$且 $P=\mathrm{col}(a)$。由 $a=a^2$ 知$(a^*)^2=a^*$。记 $I=I_n$(n 阶单位方阵),则

$$(I-2a)(I-2a^*)=(I-2a)(I-2a)^*$$

为半正定 Hermite 矩阵。于是有 $g=g^*\in GL_n(C(X))$使

$$g^2=I+(I-2a)(I-2a^*)$$

(补成正定 Hermite 矩阵,再开方)。由此知

$$
\begin{aligned}
(I+(I-2a)(I-2a^*))a^* &= 2a^* - 2a^{*2} - 2aa^* + 4aa^* \\
&= 2a^* - 2a^* - 2aa^* + 4aa^* \\
&= 2aa^* \\
&= a(I+(I-2a)(I-2a^*))
\end{aligned}
$$

即

$$
g^2 a^* = a g^2 \tag{1}
$$

由(1)知,

$$
g a^* g^{-1} = g^{-1} a g \tag{2}
$$

记 $e=g^{-1}ag$,则

$$
\begin{aligned}
e^2 &= g^{-1}a^2 g = g^{-1} a g = e \\
e^* &= g a^* g^{-1} \overset{}{\underset{(2)}{=\!=}} g^{-1} a g \\
&= e
\end{aligned}
$$

即,e 为 C(X)上的 n 阶 Hermite 矩阵。显然,作为${}_{C(X)}\mathfrak{M}$,

$$
P = \mathrm{col}(a) \simeq \mathrm{col}(e)
$$

□

引理 14.2 $\forall P \in$ f. g. $\mathrm{P}_{C(X)}\mathfrak{M}$,$P$ 给出 X 上的向量丛 $\Gamma^*(P)=X\times P \in \mathcal{V}ec(X)$且纤维都是 f. g. $\mathrm{Free}_F\mathfrak{M}$。

证 由引理 14.1 知,可令 $P\oplus Q=C(X)^n$,$e^2=e=e^*\in C(X)^{n\times n}$且 $P=\mathrm{col}(e)$。作映射

$$
\begin{aligned}
\varphi: X\times C(X)^n &\to X\times F^n, \\
(x, f_1, \cdots, f_n) &\mapsto (x, f_1(x), \cdots, f_n(x))
\end{aligned}
$$

由 F 按度量给出的拓扑及 X 的拓扑给出 $X\times F^n$ 的拓扑。再通过取映射 φ 的原象又给出 $X\times C(X)^n$ 的拓扑。于是 $\Gamma^*(P)=X\times P$ 为一个拓扑空间且为 X 上的一个向量丛(其局部平凡性将在下面引理 4.14 之证中顺便给出),它在 $x\in X$ 的纤维为 $e(x)F^n$(当然是有限生成自由 F-模),其中 $e(x)$ 为 $e\in C(X)^{n\times n}$在 x 点的值。 □

引理 14.3 设 $e^2=e\in C(X)^{n\times n}$,$x,y\in X$,则 $e(x)^2=e(x)\in F^{n\times n}$且

$$
g \equiv e(x)e(y) + (I_n - e(x))(I_n - e(y)) \in \mathrm{GL}_n(F),
$$

且 $e(x)$与 $e(y)$在 F 上是 g 相似的:$g^{-1}e(x)g=e(y)$。

证 在前面的记号下,$P\in$ f. g. $\mathrm{P}_{C(X)}\mathfrak{M}$ 对应的 $e=e^2=e^*\in C(X)^{n\times n}$(即 e 为 C(X)上的幂等的 Hermite 矩阵)。$P\simeq\mathrm{col}(e)$。记

$$
Y_1 = \{p^2 = p = p^* \in F^{n\times n}\}
$$

定义 p 的范数为(对 $z=(z_1,\cdots,z_n)\in F^n$,用 z 的向量范数$|z|=\Sigma z_j^* z_j$)

$$
\| p \| = \sup_{|z|=1, z\in F^n} | pz |
$$

由 $p(p-1)=0$ 知 p 的特征值 $\lambda_p=0,1$，因此 $\|p\|\leqslant 1$，$\forall p\in Y_1$。于是 Y_1 为紧致的 Hausdorff 空间。对 $\forall f:Y_1\to I=[0,1]$，称

$$\operatorname{supp} f \equiv \overline{\{y\in Y_1 \mid f(y)\neq 0\}}(\overline{\{\ \}}\text{ 表示}\{\}\text{ 的闭包})$$

为 f 的支撑。回顾单位分解的定义：设 Y 为拓扑空间，$\{f_\alpha:Y\to I$ 连续$\}$称为 Y 上的**单位分解**(partition of unity on Y)是指：(1) $\{\operatorname{supp} f_\alpha\}$为 Y 的局部有限闭覆盖；(2) $\sum\limits_\alpha f_\alpha(y)=1$，$\forall y\in Y$(此是有限和，因为由(1)，$y$ 仅在有限个支撑中)。若$\{U_\alpha\}$为 Y 的开覆盖使 $\operatorname{supp} f_\alpha\subseteq U_\alpha$，则称$\{f_\alpha:Y\to I$ 连续$\}$为从属于$\{U_\alpha\}$的单位分解。(当 Y 为仿紧 Hausdorff 空间时，对 Y 的每一开覆盖都有从属于它的单位分解)。

于是由 Y_1 的紧致性知，在 Y_1 上有有限的单位分解 $S'=\{f_1',\cdots,f_k'\}$，因此，$\forall p,q\in Y_1$，当有 $f_j'\in S'$ 使 $f_j'(p)f_j'(q)\neq 0$ 时，通过加细开覆盖(总有从属于它们的单位分解)知 $\|p-q\|<\frac{1}{3}$。但由

$$\begin{aligned} e:X &\to Y_1 \\ x &\mapsto e(x) \end{aligned}$$

连续知 S'给出 X 上的单位分解 S 且在有 $f\in S$ 使 $f(x)f(y)\neq 0$ 时 $\|e(x)-e(y)\|<\frac{1}{3}$。对 $f\in S$，记

$$U(f)\equiv\{x\in X \mid f(x)\neq 0\}$$

容易验证 $e(x)g=ge(y)$对引理中的 g 成立，而 g 又可写成

$$g=I_n+(e(y)-e(x))(I_n-2e(y))$$

由于

$$\begin{aligned} \|g-I_n\| &= \|(e(y)-e(x))(I_n-2e(y))\| \\ &\leqslant \|e(y)-e(x)\|\cdot\|I_n-2e(y)\| \\ &< \frac{1}{3}\cdot 3=1 \end{aligned}$$

$\forall\lambda\in\sigma(g)$($g$ 的特征值集合，即谱集)，$|\lambda-1|<1$，因此 $\lambda\neq 0$，$\forall\lambda\in\sigma(g)$，由此知 $g\in GL_n(F)$。于是由 $e(x)g=ge(y)$知，$g^{-1}e(x)g=e(y)$。 □

引理 14.4 $\forall X\in\mathrm{Top}$，$P\in$ f. g. $P_{C(X)}\mathfrak{M}$，$F=\mathbb{R}$，$\mathbb{C}$ 或 $\mathbb{H}$，则 P 对应的 $\Gamma^*(P)=X\times P\in$ f. t. $\mathrm{Vec}(X)$。

证 由引理 14.2 已知 $\Gamma^*(P)\in\mathrm{Vec}(X)$(局部平凡性待证)且纤维都是 f. g. $\mathrm{Free}_F\mathfrak{M}$(有限维 F-线性空间)。由 f. t. $\mathrm{Vec}(X)$的定义与上引理之证知，只需再证其局部平凡性。

事实上，在上述记号下，$\forall x\in U(f)$，已知有 $g\in GL_n(F)$，使得 $e(y)=$

$g^{-1}e(x)g$，其中 $y\in X$ 使 $\| e(x)-e(y) \| < \frac{1}{3}$。由 F 为 $\mathbb{R}$ 上的可除代数知，$\forall z\in X$，

$$\mathrm{col}(e(z)) \in {}_F\mathfrak{M} \quad 且 \quad \dim_F \mathrm{col}(e(z)) < \infty$$

因此

$$\mathrm{col}(e|_{U(f)}) \in \mathrm{f.g.Free}_{C(U(f))}\mathfrak{M}$$

即 $\Gamma^*(p)|_{U(f)}$ 是平凡的。于是 $\Gamma^*(P)\in \mathrm{f.t.Vec}(X)$。 □

引理 14.5 $\forall \xi=(E,p,X)\in \mathrm{f.t.Vec}(X)$，其截面集 $\Gamma(\xi)\in \mathrm{f.g.P}_{C(X)}\mathfrak{M}$。

证 由设与定义 14.2，可令 S 为 X 上的单位分解且使：$\forall f\in S$，有 $U(f)$ 使 ξ 在 $U(f)$ 上是平凡的。

对任意的 $f\in S$，记 $a_1(f),\cdots,a_n(f)$ 为 $\Gamma(\xi)|_{U(f)}$ 的基（$n=n(f)$）。下面我们将此基“开拓”为 $\Gamma(\xi)$ 的生成系。

$\forall g\in S$，记

$$a_j(f) = \Sigma c_{ij}(f,g)a_i(g)$$

在 $U(f)\cap U(g)$ 上显然有 $f'\in C(X)$ 使 $f'\geqslant 0$ 且与 f 有相同的零点（取 $f'=|f|$ 即可）且在 $U(f)\cap U(g)$ 上 $f(x)\to 0$ 时，$c_{ij}(f,g)f'\to 0$，$\forall i,j,g$。于是

$$b_j(f) = \begin{cases} a_j(f)f', & 在\ U(f)\ 上 \\ 0, & 在\ X\backslash U(f)\ 上 \end{cases}$$

为此丛的一个连续的（整体）截面且

$$\{b_j(f)|_{U(f)},\ 1\leqslant j\leqslant n\}$$

为 $\Gamma(\xi)|_{U(f)}$ 之基。下面来证：$\{b_j(f)\,|\,1\leqslant j\leqslant n, f\in S\}$ 为 $\Gamma(\xi)\in {}_{C(X)}\mathfrak{M}$ 的生成系。

$\forall s\in\Gamma(\xi)$，记 $\xi|_{U(f)}=\Sigma c_j(f)b_j(f)$，$\forall c_j(f)\in C(U(f))$

用 S 修改单位分解 S 使 X 的开覆盖 $\{U(f)\,|\,f\in S\}$ 保持不变，但对修改后的单位分解满足：$f\to 0$ 时，$c_j(f)f\to 0$（在 $U(f)$ 上）。为此定义

$$d_j(f) = \begin{cases} c_j(f)f, & 在\ U(f)\ 上 \\ 0, & 在\ X\backslash U(f)\ 上 \end{cases}$$

则 $d_j(f)\in C(X)$，且

$$s = \sum_{f\in S}\sum_{j=1}^{n(f)} d_j(f)b_j(f)$$

因此 $\{b_j(f)\,|\,1\leqslant j\leqslant n=n(f), f\in S\}$ 为 $\Gamma(\xi)\in {}_{C(X)}\mathfrak{M}$ 的生成系。

记 $N=\sum_{f\in S}n(f)$（$\Gamma(\xi)$ 的生成元个数），则由 $|S|<\infty$ 知 $N<\infty$。注意 $F=\mathbb{R},\mathbb{C}$ 或 $\mathbb{H}$ 时，在 $C(X)^N$ 上可定义正定 Hermite 矩阵 $A=A^*\in$

$C(X)^{N\times N}$，于是有满同态

$$\psi: C(X)^N \longrightarrow \Gamma(\xi)$$

$$(g_1,\cdots,g_N) \longmapsto (\bar{g}_1,\cdots,\bar{g}_N)A(b_1(f),\cdots,b_N(f))^T$$

容易看出（注意 $A\in GL_N(C(X))$）ψ 是可分裂的（$0\to\mathrm{Ker}\psi\to C(X)^N\to\Gamma(\xi)\to 0$ 可裂），因此 $\Gamma(\xi)\in$ f. g. $P_{C(X)}\mathfrak{M}$。 □

定理 14.1 之证　容易看出引理 14.4 与引理 14.5 给出的 Γ^*，Γ 为互逆函子，

$$\text{f. g. } P_{C(X)}\mathfrak{M} \underset{\Gamma^*}{\overset{\Gamma}{\rightleftarrows}} \text{f. t. } \mathcal{V}ec(X),$$

因此 f. t. $\mathcal{V}ec(X)$ 与 f. g. $P_{C(X)}\mathfrak{M}$ 为等价范畴。又 Γ 变 f. t. $\mathcal{V}ec(X)$ 的 Whitney 和为 f. g. $P_{C(X)}\mathfrak{M}$ 的直和，而 Γ^* 变 f. g. $P_{C(X)}\mathfrak{M}$ 的直和为 f. t. $\mathcal{V}ec(X)$ 的 Whitney 和。由注①又知 Γ，Γ^* 都保持 $\otimes$ 的对应。因此可知 f. t. $K_F^0(X)\simeq K_0(C(X))$（是 Abel 群同构，也是（交换）环同构）。 □

注意到当 X 为紧致的 Hausdorff 空间时，$\mathcal{V}ec(X)$ 即 f. t. $\mathcal{V}ec(X)$，因此由定理 14.1 立得

定理 14.2（Swan，1962）　设 X 为紧致的 Hausdorff 空间，$F=\mathbb{R}$，$\mathbb{C}$ 或 $\mathbb{H}$（实四元数体），则 $\mathcal{V}ec(X)$ 与 f. g. $P_{C(X)}\mathfrak{M}$ 是等价范畴。因此

$$K_F^0(X)\simeq K_0(C(X)),$$

其中 $C(X)$ 为 X 到 F 的连续函数环。上述的同构是 Abel 群同构，也是（交换）环同构。

第四章　范畴的 K_0 群及 K_1 群的正合列

在本章中我们将在范畴论的高度来研究 K_0 群与 K_1 群。先定义带正合列范畴的 K_0 群与 K_1 群，用于有限生成投射 R-模范畴 f. g. $P_R\mathfrak{M}$，证明了 $K_0(R)$ 与 K_0(f. g. $P_R\mathfrak{M}$)的同构性，用于有限生成 R-模范畴 f. g. ${}_R\mathfrak{M}$ 定义了 G_0 群 $G_0(R)$ 与 G_1 群 $G_1(R)$。在 R 为左(同调)正则环时，证明了 $K_i(R)\simeq G_i(R)$，$i=0,1$。对 Descartes 方图，研究了其中的几个环上的有限生成投射模范畴之间的关系，由此得出有重要应用的 K_0 群与 K_1 群的六项正合列(Mayer-Vietoris 列)。在§18 中介绍了代数数论中的一个重要课题——分圆域的类数计算的进展情况，且作为上述六项正合列的应用，给出这方面有用的结果(见命题 18.3)。

§15　带正合列范畴的 K_0 群与 K_1 群

在前面诸节中，我们已多次使用过范畴等术语。所谓范畴 $\mathscr{C}$ 是指一个系统。它有三个组成(对象类，每两个对象 A,B 间的态射集 $\mathrm{Hom}_{\mathscr{C}}(A,B)$(可以是空集)，以及态射 $\alpha\in\mathrm{Hom}_{\mathscr{C}}(A,B)$，$\beta\in\mathrm{Hom}_{\mathscr{C}}(B,C)$ 的合成 $\beta\alpha\in\mathrm{Hom}_{\mathscr{C}}(A,C)$)并满足三个公理：$C_1$：$\mathrm{Hom}_{\mathscr{C}}(A,B)\cap\mathrm{Hom}_{\mathscr{C}}(C,D)=\varnothing$，$\forall A\neq C$ 或 $B\neq D$；C_2：态射的合成满足结合律；C_3：$\forall A\in\mathscr{C}$，$\exists I_A\in\mathrm{Hom}_{\mathscr{C}}(A,A)$(恒等态射)与可合成的态射左、右合成时起单位元的作用。

如果 $\mathscr{C}$ 有零对象 0(即 $\forall A\in\mathscr{C}$，$\mathrm{Hom}_{\mathscr{C}}(0,A)$ 与 $\mathrm{Hom}_{\mathscr{C}}(A,0)$ 都只有一个态射)且对 $\forall A,B\in\mathscr{C}$，$\mathrm{Hom}_{\mathscr{C}}(A,B)$ 都是加法 Abel 群，且加法与态射的合成满足分配律，则称 $\mathscr{C}$ 为**预加法范畴**(pre-additive category)。

预加法范畴 $\mathscr{C}$ 若又满足：$\forall$ 有限个 $A_1, A_2, \cdots, A_n \in \mathscr{C}$，必有直和 $\coprod_{j=1}^{n} A_j$（直积 $\prod_{j=1}^{n} A_j$），则 $\mathscr{C}$ 称为**加法范畴**(additive category)。

加法范畴 $\mathscr{C}$ 若又满足

A_1：$\mathscr{C}$ 中任何态射 f 都有核 $\mathrm{Ker} f$ 与上核 $\mathrm{Coker} f$；

A_2：$\mathscr{C}$ 中的单态射(左可消态射)都是其上核的核，$\mathscr{C}$ 中的满态射(右可消态射)都是其核的上核；

A_3：$\mathscr{C}$ 中任意态射 σ 都可分解为 $\sigma = \eta\pi$，其中 η 为单态射(也称为 σ 的像，记为 $\mathrm{Im}\sigma$)，π 为满态射(也称为 σ 的余像，记为 $\mathrm{Coim}\sigma$)，则称 $\mathscr{C}$ 为 **Abel 范畴**。其中态射 f 的核为 i，是指：$fi = 0$ 且 i 具有泛性质；若 $fg = 0$，则必有惟一的态射 τ 使 $i\tau = g$，上核的定义是对偶的。

在 Abel 范畴中，可定义正合列(一个态射列 $\cdots \to A_{j-1} \xrightarrow{f_{j-1}} A_j \xrightarrow{f_j} A_{j+1} \to \cdots$ 为正合列，指 $\forall j, \mathrm{Im} f_{j-1} = \mathrm{Ker} f_j$)。

在本书中我们用得最多的是 $_R\mathfrak{M}$(包括 $_Z\mathfrak{M}$ 即 $\mathcal{A}G$)，这是最典型的 Abel 范畴。本节中我们立足于 Abel 范畴的一种子范畴(称 $\mathscr{D}$ 为 $\mathscr{C}$ 的**子范畴**是指 $\mathscr{D}$ 中的对象都是 $\mathscr{C}$ 中的对象且 $\mathrm{Hom}_{\mathscr{D}}(A, B) \subseteq \mathrm{Hom}_{\mathscr{C}}(A, B)$，$\forall A, B \in \mathscr{D}$. 当这里的等号总成立时又称 $\mathscr{D}$ 为 $\mathscr{C}$ 的**全子范畴**(full subcategory))。先给出这种子范畴的严格定义。读者也可按 $_R\mathfrak{M}$ 去理解或参看[佟文廷，1998]。

定义 15.1 设 $\mathscr{A}$ 为 Abel 范畴，$\mathscr{P}$ 为 $\mathscr{A}$ 的全加法子范畴(即 $\mathscr{P}$ 为 $\mathscr{A}$ 的全子范畴且 $\mathscr{P}$ 又为加法范畴)且满足下述两个条件：

(E_1) $\mathscr{P}$ 对扩张封闭，即对 $\mathscr{A}$ 中任一短正合列

$$0 \to P_1 \to P \to P_2 \to 0,$$

若 $P_1, P_2 \in \mathscr{P}$，则 $P \in \mathscr{P}$；

(E_2) $\mathscr{P}$ 有**小骨干**(small skeletal)**子范畴** $\mathscr{P}_0$，即 $\mathscr{P}_0$ 为 $\mathscr{P}$ 的全子范畴且为**小范畴**(对象类为集合)。同时对任意的 $P \in \mathscr{P}$ 必有相应的 $Q \in \mathscr{P}_0$ 使 $P \simeq Q$($\mathscr{P}$ 中的等价(同构))，则称 $\mathscr{P}$ 为**带正合列范畴**(category with exact sequences)**或正合范畴**(exact category)。这里的正合列指 $\mathscr{A}$ 中的正合列，其中的对象与态射都是 $\mathscr{P}$ 中的对象与态射。

由于定义 15.1 是本节的立足点，需举几个例子使读者能较清楚地理解这个定义。

例 1 一切小 Abel 范畴都是带正合列范畴(如除环上的有限维线性空间范畴，但 $_R\mathfrak{M}$ 非小 Abel 范畴甚至 $_Z\mathfrak{M}$ 也非小 Abel 范畴)。更一般地，具有小骨干子范畴的 Abel 范畴也是带正合列范畴(如拓扑群 G 的有限维复表

示范畴，其小骨干为$\{\mathrm{Hom}(G,\mathrm{GL}_n(\mathbb{C}))\mid n\in\mathbb{N}\}$。

例 2 f. g. $\mathrm{P}_R\mathfrak{M}$（因此紧致 Hausdorff 空间 X 上的$\mathcal{V}ec(X)$，拓扑空间 Y 上的有限型向量丛范畴 f. t. $\mathcal{V}ec(Y)$）是带正合列范畴，其小骨干为 $\mathscr{P}_0=\{R^n$ 之直和项$\mid n\in\mathbb{N}\}$且短正合列都可裂。但 f. g. $\mathrm{P}_R\mathfrak{M}$ 与 $\mathscr{P}_0$ 非 Abel 范畴，因为有限生成投射模之间的同态之上核未必为投射的，比如 $R=\mathbb{Z}$ 时，$\begin{array}{c}\mathbb{Z}\xrightarrow{2}\mathbb{Z}\\ m\mapsto 2m\end{array}$之上核为$\mathbb{Z}_2\notin\mathrm{P}_Z\mathfrak{M}$。

例 3 f. g. ${}_R\mathfrak{M}$ 是带正合列范畴，其小骨干为 $\mathscr{P}_0=\{R^n$ 的商模（同态象）$\mid n\in\mathbb{N}\}$。但 R 非 Noether 环时，f. g. ${}_R\mathfrak{M}$ 非 Abel 范畴（有限生成模之间的同态核未必为有限生成的，比如 $f\colon R\to R/I, I\lhd R, \mathrm{Ker}f=I$ 未必为有限生成的）。因此带正合列范畴未必为 Abel 范畴，尽管它们必是 Abel 范畴的一种全子范畴。

建议读者补证 f. g. ${}_R\mathfrak{M}$ 对扩张封闭。

例 4 记有有限投射分解的 R-模范畴

$$\text{f. p. r}_R\mathfrak{M}=\{M\in{}_R\mathfrak{M}(\text{f. g. }{}_R\mathfrak{M})\mid 0\to P_n\to\cdots\to P_0\to M\to 0\text{ 正合}\\ P_j\in\text{f. g. P}_R\mathfrak{M}, n=n(M)\}$$

显然 f. p. r. ${}_R\mathfrak{M}$ 为 f. g. ${}_R\mathfrak{M}$ 的全子范畴也是${}_R\mathfrak{M}$ 的全子范畴。用马掌引理（见[佟文廷，1998]），可证 f. p. r. ${}_R\mathfrak{M}$ 满足(E_1)，由例 3 知它又满足(E_2). 因此 f. p. r. ${}_R\mathfrak{M}$ 为带正合列范畴且为 f. g. ${}_R\mathfrak{M}$ 的全加法子范畴。当 R 为左（同调）正则环（即 R 为（左）Noether 环且 $\mathrm{lpd}M<\infty$, $\forall M\in$ f. g. ${}_R\mathfrak{M}$，比如 $R\in\mathrm{PID}$, R 为 Dedekind 环，更一般地，当 R 为左 Noether 环且 $\mathrm{lgD}(R)<\infty$ 时，R 都是左（同调）正则环）时，f. p. r. ${}_R\mathfrak{M}=$ f. g. ${}_R\mathfrak{M}$。

建议读者研究一下，有限表示 R-模范畴

$$\text{f. p. }{}_R\mathfrak{M}=\{M\in{}_R\mathfrak{M}\mid\exists m=m(M), n=n(M)\text{ 使 }R^m\to R^n\to M\to 0\text{ 正合}\}$$

是否为带正合列范畴?

对带正合列范畴可定义 K_0 群与 K_1 群。

定义 15.2 设 $\mathscr{P}$ 为带正合列范畴，$\mathscr{P}_0$ 为其小骨干子范畴。记 $\mathrm{K}_0(\mathscr{P})$ 为以 $\mathscr{P}_0$ 中对象作基的自由 Abel 群按下述运算关系所得的 Abel 群（$[P]$表示对应于 $P\in\mathscr{P}_0$ 的 $\mathrm{K}_0(\mathscr{P})$元素）：

$(1)_{\mathrm{K}_0}$：在 $\mathscr{P}$ 中若 $P\simeq P'$，则$[P]=[P']$；

$(2)_{\mathrm{K}_0}$：对 $\mathscr{P}$ 中任意的短正合列 $0\to P_1\to P\to P_2\to 0$，

$$[P]=[P_1]+[P_2]$$

（注意$(2)_{\mathrm{K}_0}\Rightarrow(1)_{\mathrm{K}_0}$：令 $P_1=0$ 即知），

称 $K_0(\mathscr{P})$ 为 $\mathscr{P}$ 的 K_0 群。

记 $K_1(\mathscr{P})$ 为以

$$\Omega\mathscr{P} \equiv \Omega\mathscr{P}_0 \equiv \{(P,\alpha) \mid P \in \mathscr{P}_0,$$
$$\alpha \in \mathrm{Aut}P(P\text{ 的自同构(自等价)集})\}$$

作基的自由 Abel 群按(模)下述运算关系所得的 Abel 群([(P,α)]表示对应于 (P,α) 的 $K_1(\mathscr{P})$ 元素):

$(1)_{K_1}$: $[(P,\alpha)]+[(P,\beta)]=[(P,\alpha\beta)]$;

$(2)_{K_1}$:对 $\mathscr{P}$ 中任意的行正合交换图

$$\begin{array}{ccccccccc} 0 \to & P_1 & \xrightarrow{i} & P & \xrightarrow{\pi} & P_2 & \to 0 \\ & \alpha_1\downarrow\simeq & & \alpha\downarrow\simeq & & \alpha_2\downarrow\simeq & \\ 0 \to & P_1 & \xrightarrow{i} & P & \xrightarrow{\pi} & P_2 & \to 0, \end{array}$$

$$[(P,\alpha)]=[(P_1,\alpha_1)]+[(P_2,\alpha_2)]$$

称 $K_1(\mathscr{P})$ 为 $\mathscr{P}$ 的 K_1 群,其元素$[(P,\alpha)]$常被简记为$[P,\alpha]$。

$\Omega\mathscr{P}_0$ 称为 $\mathscr{P}$(或 $\mathscr{P}_0$)的**回路范畴**(loop category),其中 $\mathrm{Hom}((P,\alpha),(P',\alpha'))=\{f \mid f\in \mathrm{Hom}(P,P')$ 且 $f\alpha=\alpha' f\}$。

记 $G_i(R)=K_i(\mathrm{f.g.}\,{}_R\mathfrak{M})$,$i=0,1$,分别称为环的 $\mathbf{G}_0$ 群与 $\mathbf{G}_1$ 群。

在证明本节的主要定理之前,先证明如下引理。

引理 15.1　设 $\mathscr{P}$ 为带正合列范畴,$\mathscr{P}_0$ 为其小骨干小范畴,则在 $K_1(\mathscr{P})$ 中,若 $\alpha^2=\alpha\in \mathrm{Aut}P$, $P\in\mathscr{P}_0$,则$[P,\alpha]=0$。特别地,$[P,I_p]=0$。

证　由$(1)_{K_1}$知

$$[P,\alpha]+[P,\alpha]=[P,\alpha^2]=[P,\alpha]$$

因此$[P,\alpha]=0$。 □

定理 15.1　设 R 为任一环,则

(1) $K_0(R)\simeq K_0(\mathrm{f.g.}\,\mathrm{P}_R\mathfrak{M})$;

(2) $K_1(R)\simeq K_1(\mathrm{f.g.}\,\mathrm{P}_R\mathfrak{M})\simeq K_0(\Omega\mathrm{f.g.}\,\mathrm{P}_R\mathfrak{M})$;

(3) 当 R 为半单 Artin 环时,

$$G_0(R)\simeq K_0(R)\simeq \mathbb{Z}^n,$$
$$G_1(R)\simeq K_1(R)\simeq V(R)(\text{见 §9})。$$

特别地,当 R 为除环时

$$G_0(R)\simeq K_0(R)\simeq \mathbb{Z},$$
$$G_1(R)\simeq K_1(R)\simeq R^{\cdot ab}$$

证　(1) 对例 2 中 Abel 范畴 $\mathscr{A}={}_R\mathfrak{M}$ 中的正合列

$$0\to P_1\to P\to P_2\to 0,$$

$P_2 \in \text{f. g. P}_R\mathfrak{M}$ 时必可裂，即 $P \simeq P_1 \oplus P_2$. 因此，$P_1, P_2 \in \mathscr{P} = \text{f. g. P}_R\mathfrak{M}$ 时 $P \in \text{f. g. P}_R\mathfrak{M}$。又 $\mathscr{P}_0 = \{R^n \text{ 的直和项} \mid n \in \mathbb{N}\}$ 为 $\mathscr{P}$ 的小骨干子范畴，$\mathscr{P}$ 为 $\mathscr{A}$ 的全加法子范畴。因此由 §1 中关于 $K_0(R)$ 的定义与定义 15.2 即得(1)。

(2) $\forall A \in GL_n(R)$，记 $\overline{A}$ 为

$$\begin{pmatrix} A & \\ & I_\infty \end{pmatrix}$$

在 $GL(R) \xrightarrow{\pi_1} GL(R)/E(R) = K_1(R)$ 之下的象，则 A 确定一个 $\alpha \in \text{Aut}R^n$。令

$$\varphi: K_1(R) \to K_1(\text{f. g. P}_R\mathfrak{M}),$$
$$\overline{A} \mapsto [R^n, \alpha]$$

来证 φ 为群同构。

(i) φ 为完全确定的群同态

若在 $K_1(R)$ 中

$$\overline{A}_1 = \pi_1 \begin{pmatrix} A_1 & \\ & I_\infty \end{pmatrix} = \overline{A}, \qquad A_1 \in GL_{n_1}(R)$$

A_1 确定的 $\alpha_1 \in \text{Aut}R^{n_1}$，则有 $N \geqslant n, n_1$ 使

$$\overline{A \oplus I_{N-n}} = \overline{A_1 \oplus I_{N-n_1}}$$

但在 $K_1(\text{f. g. P}_R\mathfrak{M})$ 中，由 $(2)_{K_1}$ 知

$$[R^{N-n}, I_{N-n}] + [R^n, \alpha] = [R^N, \alpha \oplus I_{N-n}]$$

(考察行正合交换图

$$\begin{array}{ccccccccc} 0 \to & R^n & \xrightarrow{i} & R^N & \xrightarrow{\pi} & R^{N-n} & \to 0 \\ & \downarrow \alpha & & \downarrow \alpha \oplus I_{N-n} & & \downarrow I_{N-n} & \\ 0 \to & R^n & \xrightarrow{i} & R^N & \xrightarrow{\pi} & R^{N-n} & \to 0) \end{array}$$

而由引理 15.1 又知 $[R^{N-n}, I_{N-n}] = 0$，因此

$$[R^n, \alpha] = [R^N, \alpha \oplus I_{N-n}]$$

同理知

$$[R^{n_1}, \alpha_1] = [R^N, \alpha_1 \oplus I_{N-n_1}]$$

因此不失一般地对 $\forall \overline{B}, \overline{C} \in K_1(R)$，令 $B \in GL_N(R)$ 对应(确定) $\beta \in \text{Aut}R^N$，$C \in GL_N(R)$ 对应 $\gamma \in \text{Aut}R^N$，则 $BC \in GL_N(R)$ 对应 $\gamma\beta \in \text{Aut}R^N$ (矩阵写在 $R^{1 \times N}$ 中向量之右边)。于是在上述记号下，

$$\varphi(\overline{B} \cdot \overline{C}) = \varphi(\overline{BC}) = [R^N, \gamma\beta]$$
$$\xlongequal[(1)_{K_1}]{} [R^N, \gamma] + [R^N, \beta] = \varphi(\overline{B}) + \varphi(\overline{C})$$

即 φ 保持群运算的对应。

为证 φ 的完全确定性，注意 $\bar{A}=\bar{A}_1$ 时必有 $C_1\in E(R)$ 使 $\bar{A}=\bar{C}_1\bar{A}_1$。于是只需证

$$\varphi(\bar{C}_1)=0,\quad 即\ \bar{C}_1=\bar{I},\forall C_1\in \mathrm{E}(R)$$

事实上，不失一般地(由 φ 保持群运算的对应)可令 $C_1=e_{ij}(a),a\in R$，对应 $\alpha_C\in \mathrm{Aut}R^N$ 由行正合交换图

$$\begin{array}{ccccccccc}0\to & R^{N-1} & \xrightarrow{i'} & R^N & \xrightarrow{\pi'} & R & \to 0\\ & \downarrow I_{N-1} & & \downarrow \alpha_C & & \downarrow I_1 & \\ 0\to & R^{N-1} & \xrightarrow{i'} & R^N & \xrightarrow{\pi'} & R & \to 0\end{array}$$

用 $(2)_{K_1}$ 知

$$\varphi(\bar{C}_1)=[R^N,\alpha_C]=[R^{N-1},I_{N-1}]+[R,I_1]\xlongequal[\text{引理 15.1}]{}0$$

(ii) φ 为群同构。

由(i)已知 φ 为群同态，再证 φ 满且单即可。

① φ 满，即 $\forall P\in \mathrm{f.g.P}_R\mathfrak{M},\alpha\in \mathrm{Aut}P,[P,\alpha]\in \mathrm{Im}\varphi$。事实上，令 $P\oplus Q=R^N$，则由 $(1)_{K_1}$ 与 $(2)_{K_1}$ 有

$$[P,\alpha]+[Q,I_Q]=[R^N,\alpha\oplus I_Q]\in \mathrm{Im}\varphi$$

但由引理 15.1 知

$$[Q,I_Q]=0$$

于是 $[P,\alpha]\in \mathrm{Im}\varphi$，即 φ 满。

② φ 单。

设 $\varphi(\bar{C})=0$ 来证 $\bar{C}=\bar{I}$ 即可，其中，$C\in \mathrm{GL}_N(R)$ 对应 $\gamma\in \mathrm{Aut}R^n$。

事实上，由 $K_1(\mathrm{f.g.P}_R\mathfrak{M})$ 的定义知(比较定理 1.1)：令 $\mathscr{F}$ 为以 $\{[P,\alpha]\mid P\in\mathscr{P}_0,\alpha\in \mathrm{Aut}P\}$ 作基的自由 Abel 群，其中 $\mathscr{P}_0$ 如例 2 所示，$\mathscr{R}$ 为由 $\{[P,\alpha]+[P,\beta,]-[P,\alpha\beta],[P,\alpha]-[P_1,\alpha_1]-[P_2,\alpha_2]\mid P,P_1,P_2\in\mathscr{P}_0,\alpha,\beta\in \mathrm{Aut}P,\alpha_j\in \mathrm{Aut}P_j$ 且有 $(2)_{K_1}$ 中的行正合交换图$\}$生成的 $\mathscr{F}$ 之子群，则

$$K_1(\mathrm{f.g.P}_R\mathfrak{M})\simeq \mathscr{F}/\mathscr{R}$$

于是 $\varphi(\bar{C})=0\Leftrightarrow[R^n,\gamma]\in\mathscr{R}$。因此只需考察 $\{R^n\mid n\in\mathbb{N}\}$，再由①之证知，可记 $\mathscr{F}$ 为 $\{[A,n]\mid A\in \mathrm{GL}_n(R),n\in\mathbb{N}\}$ 上的自由 Abel 群，且记

$$\begin{aligned}[C,n]\in\mathscr{R}=\langle\{&[A,n]+[B,n]-[BA,n],\\ &[A,n+m]-[A_1,n]-[A_2,m]\}\rangle\end{aligned}$$

$\mathscr{R}$ 中的第二类生成元由行正合交换图(A,A_1,A_2 对应的自同构仍记为 A，A_1,A_2)

$$\begin{array}{ccccccccc}0 & \to & R^n & \xrightarrow{i} & R^{n+m} & \xrightarrow{\pi} & R^m & \to & 0\\ & & \downarrow A_1 & & \downarrow A & & \downarrow A_2 & & \\ 0 & \to & R^n & \xrightarrow{i} & R^{n+m} & \xrightarrow{\pi} & R^m & \to & 0\end{array}$$

给出. 当 $m=0$ 时,此图即

$$\begin{array}{ccccccc}0 & \to & R^n & \xrightarrow{B} & R^n & \to & 0\\ & & \downarrow A_1 & & \downarrow A & & \\ 0 & \to & R^n & \xrightarrow{B} & R^n & \to & 0\end{array} \qquad B\in \mathrm{GL}_n(R),\ A_1=BAB^{-1}$$

(矩阵写在向量之右边)。$m>0$ 时,单同态 $i:R^n\to R^{n+m}$ 不失一般地可视为 R^n 到 R^{n+m} 之前 n 个 R 直和之同构嵌入。此时

$$A=\begin{pmatrix}A_1 & \\ * & A_2\end{pmatrix}$$

于是

$$[A,n+m]-[A_1,n]-[A_2,m]$$

可由

$$[A,n]-[BAB^{-1},n]$$

与

$$\left[\begin{pmatrix}A_1 & \\ * & A_2\end{pmatrix},n+m\right]-[A_1,n]-[A_2,m]$$

形的元素组合而得(取适当的基变换)。由此知,若记

$$\begin{aligned}\mathscr{R}_1\equiv\langle\{&[A,n]+[B,n]-[BA,n],\\ &[A,n]-[BAB^{-1},n]\}\rangle<\mathscr{R}\end{aligned}$$

则

$$\mathscr{F}/\mathscr{R}_1=\bigoplus_n \mathrm{GL}_n(R)^{ab}$$

(注意$[A,n]-[BAB^{-1},n]=0$ 即 $A=BAB^{-1}$,即 $AB=BA$)。再模去

$$\left\langle\left\{\left[\begin{pmatrix}A_1 & \\ * & A_2\end{pmatrix},n+m\right]-[A_1,n]-[A_2,m]\right\}\right\rangle$$

相当于在所得的

$$\varinjlim \mathrm{GL}_n(R)^{ab}=\mathrm{GL}(R)^{ab}=\mathrm{K}_1(R)$$

中模去关系

$$\overline{\begin{pmatrix}A_1 & \\ * & A_2\end{pmatrix}}=\overline{\begin{pmatrix}A_1 & \\ & A_2\end{pmatrix}}$$

但在 $\mathrm{K}_1(R)$中已有这个关系(块初等变换相当于乘 $\mathrm{E}(R)$中元素),于是 $\mathscr{R}_1$

$=\mathscr{R}$,即 $\varphi(\bar{C})=0\Leftrightarrow[R^n,\gamma]\in\mathscr{R}_1$。因此 $\varphi(\bar{C})=0$ 时 $C\in E(R)=[GL(R),GL(R)]$ 即 $\bar{C}=\bar{I}$($K_1(R)$的单位元)。

至此,我们已证出

$$K_1(R)\simeq K_1(\text{f. g. } P_R\mathfrak{M})$$

又由定义 15.2,比较 $K_0(\mathscr{P})$与 $K_1(\mathscr{P})$的定义,则知 $K_1(\text{f. g. } P_R\mathfrak{M})$即 $K_0(\Omega\text{f. g. } P_R\mathfrak{M})$添加$(1)_{K_1}$中的关系

$$[P,\alpha]+[P,\beta]=[P,\alpha\beta]$$

而得。这相当于 $K_1(R)$添加关系(记 $\bar{A}=[A]$由同构 $\varphi:\bar{A}\to[R^n,\alpha]$知)

$$[A][B]=[AB]$$

但§11 末注①对任意环 R,已证出 $K_1(R)$必有这个关系。因此

$$K_1(R)\simeq K_1(\text{f. g. } P_R\mathfrak{M})\simeq K_0(\Omega\text{f. g. } P_R\mathfrak{M})$$

(3) 由(1),(2)以及我们已知的半单 Artin 环,除环的 K_0 群,K_1 群结果即得。 □

由定理 15.1 可看出:在此定义下环的 K_1 群即 f. g. $P_R\mathfrak{M}$ 的回路范畴 Ωf. g. $P_R\mathfrak{M}$ 的 K_0 群。因此,从这个角度上来看,在代数 K 理论中 K_0 群比 K_1 群具有更重要(更基本)的意义。由定理 15.1 的证明又可得

推论 15.1 设 R 为任意环,则 $K_1(R)\simeq K_1(\text{f. g. } P_R\mathfrak{M})\simeq K_1(\text{f. g. Free}_R\mathfrak{M})$。

现在,我们给出范畴意义下的下述结果。

命题 15.1 设 $\mathscr{P}$与 $\mathfrak{M}$ 都是带正合列范畴,$F:\mathscr{P}\to\mathfrak{M}$ 为正合函子(即 F 为将 $\mathscr{P}$中短正合列变为 $\mathfrak{M}$ 中的短正合列的共变函子),则 F 诱导出群同态

$$F_i:K_i(\mathscr{P})\to K_i(\mathfrak{M}),\qquad i=0,1$$

因此 K_0,K_1 为带正合列范畴的范畴(以正合函子作态射)到 Abel 群范畴的函子。

证 注意 F 不变定义 15.2$(1)_{K_i}$,$(2)_{K_i}$,$i=0,1$(同构也对应正合列!)即得证。 □

最后,值得一提的是(参看本节的例 4),2000 年 E. N. Marcos 等在[Marcos,2000]中对弱三角 Artin 代数(weakly triangular Artinian algebra)R,(即 R 为 Artin 代数且非同构不可分解投射模全体可排序为 $P_1,\cdots,P_n$,使 $\text{Hom}_R(P_i,P_j)=0$,$\forall i>j$,比如幂等理想都有有限投射维数的代数)给出了关于 $K_0(\text{f. p. r. }_R\mathfrak{M})$的一些有趣的结果,将 M. C. R. Butler 在[Butler,1980]与 1984 年 M. Auslander 在[Auslander,1984]中关于 Artin 代数上用有限生成模范畴的 K_0 群的关系集刻画有限型性质的结果移植到这一类弱三角代数上的有限投射维数的模范畴。有兴趣的读者可将[Marcos,

2000]取来一读。

此外,[宋光天,1990]与[唐向东,2000]用不同的途径研究了半群范畴的 K_0 群,得到一系列有意义的结果。

§16 带正合列范畴的 K_i 群与 G_i 群$(i=0,1)$

本节的主要目的是给出有包含关系的带正合列范畴的 K_0 群与 K_1 群的同构(充分)条件并对(同调)正则环给出 K_i 群与 G_i 群的一致性($i=0$, 1)。为此先给出两条引理。

引理 16.1 设带正合列范畴 $\mathfrak{M}$ 为 Abel 范畴 $\mathscr{A}$ 的全子范畴,且 $\mathfrak{M}$ 对 $\mathscr{A}$ 中满态射的核封闭(即 $\mathscr{A}$ 中任意正合列 $0\to N_1\to N_2\to N_3\to 0$ 中 $N_2,N_3\in\mathfrak{M}$ 蕴含着 $N_1\in\mathfrak{M}$),则对 $\mathfrak{M}$ 中任一正合列

$$0\to M_n\to M_{n-1}\to\cdots\to M_1\to M_0\to 0,\qquad(1)$$

$$\sum_{j=0}^{n}(-1)^j[M_j]=0\in K_0(\mathfrak{M})。$$

证 由定义 15.2 知,$(1)_{K_0}$ 蕴含着 $n=1$ 时引理成立,$(2)_{K_0}$ 蕴含着 $n=2$ 时,引理成立。

令 $n\geqslant 3$,对 n 用归纳法,设 $n\leqslant m-1$ 时引理成立。注意

$$K=\mathrm{Ker}(M_1\twoheadrightarrow M_0)\in\mathfrak{M}$$

原正合列(1)可拆成两个正合列:

$$0\to K\to M_1\to M_0\to 0,$$

$$0\to M_n\to M_{n-1}\to\cdots\to M_2\to K\to 0。$$

由归纳假设知

$$[K]+[M_0]=[M_1]$$

且

$$[K]-\sum_{j=2}^{n}(-1)^j[M_j]=0$$

将此二式合起来,即知引理成立。 □

由此引理立得

推论 16.1 (命题 1.5) 在 $\mathrm{f.g.}\,P_R\mathfrak{M}$ 中,若有正合列

$$0\to P_n\to P_{n-1}\to\cdots\to P_1\to P_0\to 0,$$

则

$$\sum_{j=0}^{n}(-1)^j[P_j]=0\in K_0(R)$$

引理 16.2　设两个带正合列范畴 $\mathfrak{M}$ 与 $\mathscr{P}$ 都是 Abel 范畴 $\mathscr{A}$ 的全子范畴，且 $\mathscr{P}$ 为 $\mathfrak{M}$ 的全子范畴。同时，$\mathscr{P},\mathfrak{M}$ 满足：

(1) $\forall M\in\mathfrak{M}$，M 都有有限长的 $\mathscr{P}$ 分解，即有 $\mathfrak{M}$ 中的正合列

$$0\to P_n\to P_{n-1}\to\cdots\to P_0\xrightarrow{\varepsilon}M\to 0,\qquad(2)$$

其中 $P_j\in\mathscr{P},j=0,1,\cdots,n$；

(2) 若 $0\to M_1\to M_2\to M_3\to 0$ 为 $\mathscr{A}$ 中的短正合列，则 $M_2,M_3\in\mathfrak{M}(\mathscr{P})$ 蕴含着 $M_1\in\mathfrak{M}(\mathscr{P})$，即 $\mathfrak{M}$ 与 $\mathscr{P}$ 都对 $\mathscr{A}$ 中满态射的核封闭，则对 $\mathfrak{M}$ 中任意态射 $\alpha:M'\to M$ 及 M 的形如(2)的有限 $\mathscr{P}$ 分解(2)，必有行为有限 $\mathscr{P}$ 分解的交换图(复形理论中比较定理的模拟，参看[佟文廷，1998])：

$$\begin{array}{ccccccccccc}0\to\cdots\to & P'_{n+1} & \to & P'_n & \to\cdots\to & P'_0 & \xrightarrow{\varepsilon'} & M' & \to 0\\ & \downarrow 0 & & \downarrow\alpha_n & & \downarrow\alpha_0 & & \downarrow\alpha & \\ & 0 & \to & P_n & \to\cdots\to & P_0 & \xrightarrow{\varepsilon} & M & \to 0\end{array}$$

证　由 $\varepsilon:P_0\twoheadrightarrow M$ 为满态射知，$(\varepsilon,-\alpha):P_0\oplus M'\twoheadrightarrow M$ 为满态射。再由条件(2)(注意由 $\mathfrak{M}$ 对扩张的封闭性，见定义 15.1$(E)_1$，$P_0\oplus M'\in\mathfrak{M}$)，在 $\mathfrak{M}$ 中必有 $\mathrm{Ker}(\varepsilon,-\alpha):B\to P_0\oplus M'$(即 ε 与 α 的拉回图(参见§13，例 11，由 ε 满知 $\beta:B\twoheadrightarrow M'$ 满)：

$$\begin{array}{ccc}B & \xrightarrow[\beta]{} & M'\\ \downarrow\gamma & \lrcorner & \downarrow\alpha\\ P_0 & \xrightarrow[\varepsilon]{} & M\end{array}$$

又由条件(1)知(注意 $B\in\mathfrak{M}$)，必有满态射 $P'_0\twoheadrightarrow B,P'_0\in\mathscr{P}$。将此与 β 合成得满态射 $\varepsilon':P'_0\twoheadrightarrow M'$；将此与 γ 合成得态射 $\alpha_0:P'_0\to P_0$。注意 ε',ε 都有核，分别记为 K'_0,K_0，则 $K'_0,K_0\in\mathfrak{M}$。再由条件(1)又知有满态射 $P'_1\twoheadrightarrow K'_0,P_1\twoheadrightarrow K_0$，其中 $P'_1,P_1\in\mathscr{P}$. 记它们的核各为 $K'_1,K_1\in\mathfrak{M}$。用归纳法，设已得行正合交换图

$$\begin{array}{ccccccccc}0\to & K'_{j-1} & \to & P'_{j-1} & \to\cdots\to & P'_0 & \xrightarrow{\varepsilon'} & M' & \to 0\\ & \downarrow\sigma & & \downarrow\alpha_{j-1} & & \downarrow\alpha_0 & & \downarrow\alpha & \\ 0\to & K_{j-1} & \to & P_{j-1} & \to\cdots\to & P_0 & \xrightarrow{\varepsilon} & M & \to 0,\end{array}$$

其中 $P_i,P'_i\in\mathscr{P}(i=0,1,\cdots,j-1)$ 且态射 $\sigma:K'_{j-1}\to K_{j-1}$ 为 α_{j-1} 在 K'_{j-1} 上的限制。重复上述步骤得行正合交换图

$$\begin{array}{ccc} P_j' & \longrightarrow K_{j-1}' \to 0 \\ \downarrow \alpha_j & \downarrow \sigma \\ P_j & \longrightarrow K_{j-1} \to 0 \end{array}$$

由归纳法即得 $\mathfrak{M}$ 中的行正合交换图

$$\begin{array}{ccccccc} 0 \to K_n' \to P_n' \to \cdots \to P_0' & \xrightarrow{\varepsilon'} & M' \to 0 \\ \downarrow \alpha_n \qquad \downarrow \alpha_0 & & \downarrow \alpha \\ 0 \to P_n \to \cdots \to P_0 & \xrightarrow{\varepsilon} & M \to 0, \end{array}$$

其中 $P_j, P_j' \in \mathscr{P}, j=0,1,\cdots,n$。最后由条件(1)用于 $K_n' \in \mathfrak{M}$ 即得证。 □

由此引理可得如下推论,该推论可用于 $K_0(R)$(令 R 为左(同调)正则环且 $\mathscr{P}=\mathrm{f.\,g.\,P}_R\mathfrak{M}, \mathfrak{M}=\mathrm{f.\,g.}\,{}_R\mathfrak{M}, \mathscr{A}={}_R\mathfrak{M}$),从而可知在 $M \in \mathrm{f.\,g.}\,{}_R\mathfrak{M}$ 的有限生成投射分解(2)中

$$\sum_{j=0}^{n}(-1)^j[P_j]$$

为 M 确定的不变量。

推论 16.2 在引理 16.2 的条件下,若 $M \in \mathfrak{M}, P. \xrightarrow{\varepsilon} M$, $P'. \xrightarrow{\varepsilon'} M$ 为 M 的两个有限 $\mathscr{P}$ 分解,则在 $K_0(\mathscr{P})$ 中

$$\sum_j(-1)^j[P_j] = \sum_j(-1)^j[P_j'] \equiv \chi(M)(M \text{ 的 Euler 示性数})。$$

证 由引理 16.2 知,有 M 的有限 $\mathscr{P}$ 分解作上行的行正合交换图

$$\begin{array}{ccccc} 0 \to P''_n & \xrightarrow{d''_n} \cdots \to P''_0 & \xrightarrow{\varepsilon''} & M \to 0 \\ (\alpha_n, \alpha_n') \downarrow & (\alpha_0, \alpha_0') \downarrow & & \Delta \downarrow \\ 0 \to P_n \oplus P_n' & \xrightarrow{d_n \oplus d_n'} \cdots \to P_0 \oplus P_0' & \xrightarrow{\varepsilon \oplus \varepsilon'} & M \oplus M \to 0, \end{array}$$

其中 $\Delta=(I_m, I_m)$ 为对角态射。记$(C.,\delta)$为复形链态射 $\alpha.:P''.\to P.$ 的态射锥(也是复形),即 $C_n=P''_{n-1}\oplus P_n$(因此$\in \mathscr{P}$, $\forall n$),而

$$\delta_n(p'',p) = (-d''_{n-1}(p''), \alpha(p'') + d_n(p))$$

于是有 $\mathscr{P}$ 上复形的短正合列

$$0 \to (P.,d) \to (C.,\delta) \to P''_{.-1},\ d'') \to 0$$

以及由此给出的长正合列(注意足码!)

$$\cdots \to \mathrm{H}_{n-1}(P''.) \xrightarrow{\delta_{n-1}} \mathrm{H}_{n-1}(P.) \to \mathrm{H}_{n-1}(C.) \to$$

$$\to H_{n-2}(P''.) \xrightarrow{\delta_{n-2}} H_{n-2}(P.) \to \cdots$$

容易验知 $\delta_{n-1}=H_{n-1}(\alpha)\equiv\alpha_*$ 为 $\mathscr{P}$ 中的同构。再注意 $H_0(P''.)\simeq H_0(P.)\simeq M$, $H_n(P''.)\simeq H_n(P.)=0$, $\forall n>1$。于是由此长正合列知 $H_n(C.)=0$, $\forall n$,即,$(C.,\delta)$为正合列。因此由引理 16.1 知,$C.$ 的 Euler 示性数 $\chi(C.)\equiv\Sigma(-1)^j[C_j]=0$。但由上述的复形短正合列(注意足码!)知 $\chi(C.)=\chi(P.)-\chi(P''.)$,于是 $\chi(P.)=\chi(P''.)$。同理知 $\chi(P'.)=\chi(P''.)$。故 $\chi(P.)=\chi(P'.)$(在 $K_0(\mathscr{P})$中),这就证出了此推论。 □

建议读者思考:取 $\mathscr{P}=\mathrm{f.g.P}_R\mathfrak{M}$, $\mathfrak{M}=\mathrm{f.g.d}_R\mathfrak{M}=\{M\in{}_R\mathfrak{M}\mid \mathrm{lpd}(M)<\infty\}$,考虑下述结论是否成立:对任意环 R, $K_0(\mathrm{f.g.P}_R\mathfrak{M})$ 为 $K_0(\mathrm{f.p.d}_R\mathfrak{M})$ 的子群。

定理 16.1 (K_0 **群的转化定理**(resolution Theorem))在引理 16.2 条件下,包含函子 $i:\mathscr{P}\to\mathfrak{M}$ 诱导一个群同构

$$i_0: K_0(\mathscr{P}) \xrightarrow[\simeq]{} K_0(\mathfrak{M})$$

证 注意 i_0 为正合函子,由命题 15.1 得群同态 i_0,使得 $i_0([P])=[P]_{\mathfrak{M}}$. 现在找出其逆同态即知 i_0 为群同构。为此,令

$$\varphi: K_0(\mathfrak{M}) \to K_0(\mathscr{P})$$

$$[M]_{\mathfrak{M}} \mapsto \sum_j(-1)^j[P_j]_{\mathscr{P}}$$

其中 $M\in\mathfrak{M}$, M 的有限 $\mathscr{P}$ 分解为

$$0\to P_n\to P_{n-1}\to\cdots\to P_0\to M\to 0$$

推论 16.2 说明 φ 与 M 的有限 $\mathscr{P}$ 分解之选取无关,因而是完全确定的群同态。由引理 16.1 知

$$[M]_{\mathfrak{M}} = \sum_j(-1)^j[P_j]_{\mathfrak{M}}$$

从而 $i_0\varphi=I_{K_0(\mathfrak{M})}$。又

$$\varphi i_0([P]_{\mathscr{P}}) = \varphi([P]_{\mathfrak{M}}) = [P]_{\mathscr{P}},\ \forall P\in\mathscr{P}$$

即 $\varphi i_0=I_{K_0(\mathscr{P})}$。因此 i_0 为群同构。 □

稍加条件(但仍能概括重要情况),又可得类似的 K_1 群转化定理。

定理 16.2 (K_1 **群的转化定理**). 设 $\mathfrak{M}$ 与 $\mathscr{P}$ 都是 Abel 范畴 $\mathscr{A}$ 中的带正合列范畴,且 $\mathscr{P}$ 为 $\mathfrak{M}$ 的全子范畴,同时它们满足:

$(1)_1$　$\forall M\in\mathfrak{M}$,有 $\mathscr{A}$ 中的满态射 $P_0\twoheadrightarrow M$,其中 $P_0\in\mathscr{P}$,使 M 的每一个自态射$(M\to M)$都能提升为 P_0 的自态射;

$(1)_2$　若

$$\cdots\to P_n\xrightarrow{d_n}P_{n-1}\to\cdots\to P_0\to M\to 0$$

为 $\mathfrak{M}$ 中的正合列,其中 $P_j \in \mathscr{P}$,则必有充分大的 n 使 $\mathrm{Ker} d_n \in \mathscr{P}$;

(2) 对 $\mathscr{A}$ 中的任意短正合列

$$0 \to M_1 \to M_2 \to M_3 \to 0,$$

$M_2, M_3 \in \mathfrak{M}(\mathscr{P})$ 蕴含着 $M_1 \in \mathfrak{M}(\mathscr{P})$,即 $\mathfrak{M}$ 与 $\mathscr{P}$ 对 $\mathscr{A}$ 中满态射的核封闭,则包含函子 $i: \mathscr{P} \to \mathfrak{M}$ 诱导 K_1 群的同构

$$i_1: \mathrm{K}_1(\mathscr{P}) \xrightarrow[\simeq]{} \mathrm{K}_1(\mathfrak{M})$$

证 容易看出,条件 $(1)_1$ 与 $(1)_2$ 蕴含着引理 16.2 中的条件(1),即 $\forall M \in \mathfrak{M}$ 都有有限 $\mathscr{P}$ 分解. 为仿定理 16.1 之证,先证明:

(i) $\forall M \in \mathfrak{M}, \alpha \in \mathrm{Aut} M$($M$ 的自同构(自等价)集),α 都可提升为 M 的一个有限 $\mathscr{P}$ 分解的自同构(自等价),即有行正合的交换图

$$\begin{array}{ccccccccccc} 0 \to & P_n & \to & P_{n-1} & \to \cdots \to & P_0 & \to & M & \to 0 \\ & \downarrow \alpha_n & & \downarrow \alpha_{n-1} & & \downarrow \alpha_0 & & \downarrow \alpha & \\ 0 \to & P_n & \to & P_{n-1} & \to \cdots \to & P_0 & \to & M & \to 0, \end{array}$$

其中 $P_j \in \mathscr{P}$,且 $\alpha_j \in \mathrm{Aut} P_j, j = 0, 1, \cdots, n$。

事实上,由 $(1)_1$ 知,可取 $P_0 \in \mathscr{P}$ 与满态射

$$P_0 \xrightarrow{\varepsilon} M$$

且使 M 的自态射都可提升为 P_0 的自态射。考察 $\alpha \oplus \alpha^{-1} \in \mathrm{Aut}(M \oplus M)$($M \oplus M$ 仍是 $\mathfrak{M}$ 的对象!)将引理 5.5 之证法(即 $\begin{pmatrix} A & \\ & A^{-1} \end{pmatrix}$ 经 $\begin{pmatrix} I & B \\ & I \end{pmatrix}$ 与 $\begin{pmatrix} I & \\ C & I \end{pmatrix}$ 形的初等块变换化为 $\begin{pmatrix} I & \\ & I \end{pmatrix}$,因此 $\begin{pmatrix} A & \\ & A^{-1} \end{pmatrix}$ 为 $\begin{pmatrix} I & B \\ & I \end{pmatrix}$, $\begin{pmatrix} I & \\ C & I \end{pmatrix}$ 形初等矩阵之积)推广到 Abel 范畴,即知:$\alpha \oplus \alpha^{-1}$ 可表为

$$\begin{pmatrix} I_M & \beta \\ & I_M \end{pmatrix} \text{与} \begin{pmatrix} I_M & \\ \gamma & I_M \end{pmatrix}$$

形的自同构之积,其中 $\beta, \gamma \in \mathrm{End} M$($M$ 的自态射集)。由 $(1)_1$ 知,β, γ 可提升为 P_0 的自态射,于是 $\alpha \oplus \alpha^{-1}$ 可提升为 $P_0 \oplus P_0$(仍是 $\mathscr{P}$ 中的对象)的自同构(关于 $\varepsilon \oplus \varepsilon, P_0 \oplus P_0 \twoheadrightarrow M \oplus M$),因此 α 可提升为 P_0 的自同构。但由条件(2)知 $\mathrm{Ker} \varepsilon \in \mathfrak{M}$,于是,重复上述作法,可得 M 的一个 $\mathscr{P}$ 分解(可能无限长)使 α 提升为此分解的自同构。最后,由条件 $(1)_2$ 知此分解可取为有限长,由此即知(i)成立。

(ii) 仿定理 16.1 之证,记包含函子 $i: \mathscr{P} \to \mathfrak{M}$ 的诱导同态为

$$i_1: \mathrm{K}_1(\mathscr{P}) \to \mathrm{K}_1(\mathfrak{M})$$

下面只需找出 i_1 的逆同态. 为此令

$$\varphi_1: K_1(\mathfrak{M}) \to K_1(\mathscr{P})$$
$$[M,\alpha] \mapsto \sum_j (-1)^j [P_j, \alpha_j],$$

其中 α_0 为 α 提升的 M 的有限 $\mathscr{P}$ 分解中的 P_0 的自同构(由(i)给出)。作范畴

$$\Omega\mathfrak{M} = \{(M,\alpha) \mid M \in \mathfrak{M}_0, \alpha \in \mathrm{Aut}M\},$$

其中 $\mathfrak{M}_0$ 为 $\mathfrak{M}$ 的小骨干子范畴且

$$\mathrm{Hom}((M,\alpha),(M',\alpha')) = \{f \mid f \in \mathrm{Hom}(M,M') \text{ 且 } f\alpha = \alpha' f\}$$

$\Omega\mathfrak{M}$ 即 $\mathfrak{M}$ 的回路范畴(loop category)。类似地作 $\mathscr{P}$ 的回路范畴

$$\Omega\mathscr{P} = \{(P,\beta) \mid P \in \mathscr{P}_0, \beta \in \mathrm{Aut}P\},$$

其中 $\mathscr{P}_0$ 为 $\mathscr{P}$ 的小骨干子范畴。用推论 16.2 于 $\Omega\mathfrak{M}$ 与 $\Omega\mathscr{P}$(易验知它们满足引理 16.2 即推论 16.2 的条件)即知 φ_1 是完全确定的(与 $\mathscr{P}$ 分解的选取无关)群同态。

再直接验证 $i_1\varphi_1 = I_{K_1(\mathfrak{M})}$,$\varphi_1 i_1 = I_{K_1(\mathscr{P})}$,即知 i_1 为群同构。 □

为了应用定理 16.1 与定理 16.2,先回忆一下同调代数中的一个重要结果(可参看[佟文廷,1998]):

设 R 为任一环,$M \in {}_R\mathfrak{M}$,则下述各点是等价的:① M 有长为 n 的投射分解;② $\mathrm{Ext}_R^{n+1}(M,-)=0$;③ $\mathrm{Ext}_R^n(M,-)$是右正合的;④ M 的长度不小于 n 的投射分解

$$\cdots \to \cdots \to P_{n+1} \to P_n \xrightarrow{d_n} \cdots \to P_0 \to M \to 0$$

中,$\mathrm{Im}d_n \in \mathrm{P}_R\mathfrak{M}$,因此可截成长为 n 的投射分解

$$0 \to \mathrm{Im}d_n \to P_{n-1} \to \cdots \to P_0 \to M \to 0$$

下面来证明

定理 16.3 设 R 为左 Noether 环,则

(1) 包含函子 i:f. g. $\mathrm{P}_R\mathfrak{M} \to$ f. p. r. ${}_R\mathfrak{M}$ 诱导的群同态

$$i_j: K_j(R) \to K_j(\text{f. p. r. } {}_R\mathfrak{M})$$

为同构,$j=0,1$;

(2) R 为左(同调)正则环时,由包含函子 i':f. g. $\mathrm{P}_R\mathfrak{M} \to$ f. g. ${}_R\mathfrak{M}$ 诱导的群同态

$$i'_j: K_j(R) \to G_j(R)$$

为同构,$j=0,1$。因此

$$K_j(R) \simeq G_j(R) \simeq K_j(\text{f. p. r}_R\mathfrak{M}),\ j = 0,1$$

证 只需验证定理 16.2 中的条件成立即可。

(1) 取 $\mathscr{P}$= f. g. $\mathrm{P}_R\mathfrak{M}$,$\mathfrak{M}$= f. p. $\mathrm{r}_R\mathfrak{M}$,$\mathscr{A} = {}_R\mathfrak{M}$,由 f. p. $\mathrm{r}_R\mathfrak{M}$ 的定义与投

射模的提升性质即知定理 16.2 中$(1)_1$ 成立。而由上段中①⇒④又知定理 16.2 中$(1)_2$ 成立。为验证定理 16.2 中的条件(2),任取 $\mathscr{A}={}_R\mathfrak{M}$ 中的正合列

$$0 \to M_1 \to M_2 \to M_3 \to 0 \tag{3}$$

$M_2, M_3 \in \mathrm{f.g.P}_R\mathfrak{M}$ 时,$M_2 \simeq M_1 \oplus M_3$。因此 $M_1 \in \mathrm{f.g.P}_R\mathfrak{M}$,当 $M_2, M_3 \in \mathrm{f.p.r}_R\mathfrak{M}$ 时可取 $n \in \mathbb{N}$ 使 M_2, M_3 的投射分解长$\leqslant n$。于是

$$\mathrm{Ext}_R^{n+l}(M_j, N) = 0, \qquad \forall N \in {}_R\mathfrak{M}, j = 2,3,\ l \geqslant 1$$

用长正合列定理得正合列

$$0 = \mathrm{Ext}_R^{n+1}(M_2, N) \to \mathrm{Ext}_R^{n+1}(M_1, N) \to \mathrm{Ext}_R^{n+2}(M_3, N) = 0$$

于是

$$\mathrm{Ext}_R^{n+1}(M_1, N) = 0,\ \forall N \in {}_R\mathfrak{M}$$

因此由上段②⇒①且注意 R 为左 Noether 环,即知 $M_1 \in \mathrm{f.p.r}_R\mathfrak{M}$,即定理 16.2 中条件(2)成立。因此本定理的结论(1)成立。

为证本定理的结论(2),仍取 $\mathscr{P}=\mathrm{f.g.P}_R\mathfrak{M}$,$\mathscr{A}={}_R\mathfrak{M}$,但 $\mathfrak{M}=\mathrm{f.g.}{}_R\mathfrak{M}$,显然定理 16.2 中的条件$(1)_1$ 成立。而由 R 为左(同调)正则环又知定理 16.2 中的$(1)_2$ 成立。由上段证明知 $\mathscr{P}=\mathrm{f.g.P}_R\mathfrak{M}$ 满足定理 16.2 中的(2),但左(同调)正则环是对左 Noether 环定义的。因此正合列(3)中的 $M_2, M_3 \in \mathfrak{M} = \mathrm{f.g.}{}_R\mathfrak{M}$ 时必有 $M_1 \in \mathfrak{M}$,即 $\mathfrak{M}$ 也满足定理 16.2 中的(2),于是本定理的结论(2)也成立。 □

由此定理可知:对左(同调)正则环 R,G_j 群及 $K_j(\mathrm{f.p.r}_R\mathfrak{M})$ 就是 $K_j(R)$,$j=0,1$,没有单独研究的必要。此外上述三条定理在其他学科(如几何学等)中有许多有趣的应用(比如对广义 Riemann-Roch 定理,Euler 示性数等),可参看[Rosenberg.1994]。值得注意的是左整体维数有限的左 Noether 环必是左(同调)正则环,但反之不然,例如 K 为域时,$R_1 = K[x_1, x_2, \cdots, x_n, \cdots]$,令 $a(n) = n(n+1)/2$,$P_n = (x_{a(n-1)+1}, x_{a(n-1)+2}, \cdots, x_{a(n)}) \lhd R_1$,$S = R_1 \setminus \bigcup\limits_{n=1}^{\infty} P_n$,则 $R = S^{-1}R_1$ 为交换 Noether 环且 Krull 维数 $\mathrm{K.dim}R = \aleph_0$,整体维数 $gD(R) = \infty$,但 R 是(同调)正则环。(见[Mcconnel,1988])。此外,我们指出:上定理中"左"改为"右"仍成立。请读者给出理由。

在本节的最后,我们简单地介绍一下由关于带正合列范畴间的正合函子产生的相对 K_0 群的一个重要应用。

设 $\mathscr{A}, \mathscr{B}$ 为两个带正合列范畴,$\mathrm{F}: \mathscr{A} \to \mathscr{B}$ 为正合函子。由上节的命题 15.1 已知,F 诱导出群同态

$$F_j: K_j(\mathscr{A}) \to K_j(\mathscr{B}), \qquad j = 0,1$$

令 $K_0(F)$ 为以

$$\{[A_0, A_1, \alpha] \mid A_j \in \mathscr{A}, \alpha \in \mathrm{Hom}_{\mathscr{A}}(A_0, A_1) \text{ 使 } F(\alpha): F(A_0) \to F(A_1) \text{ 为 } \mathscr{B} \text{ 中的同构}\}$$

作基的自由 Abel 群按下述关系所得的 Abel 群：

(1) 当 α 为 $\mathscr{A}$ 中的同构时，$[A_0, A_1, \alpha]=0$；

(2) 若有 $\mathscr{A}$ 中行正合交换图

$$\begin{array}{ccccccccc} 0 & \to & A''_0 & \to & A_0 & \to & A'_0 & \to & 0 \\ & & \downarrow \alpha'' & & \downarrow \alpha & & \downarrow \alpha' & & \\ 0 & \to & A''_1 & \to & A_1 & \to & A'_1 & \to & 0 \end{array}$$

且使 $F(\alpha), F(\alpha'), F(\alpha'')$ 都是 $\mathscr{B}$ 中的同构，则

$$[A_0, A_1, \alpha] = [A''_0, A''_1, \alpha''] + [A'_0, A'_1, \alpha']$$

称 $K_0(F)$ 为**相对(于 F 的)K_0 群**。

定义

$$\varphi: K_0(F) \to K_0(\mathscr{A})$$
$$[A_0, A_1, \alpha] \mapsto [A_0] - [A_1]$$

可验知 φ 为完全确定的群同态且 $F_0 \circ \varphi = 0$。

进一步地，再设 F 为**共尾函子**(cofinal functor，按 Bass 的定义)，即，$\forall B_1 \in \mathscr{B}$，必有 $B_2 \in \mathscr{B}$ 与 $A \in \mathscr{A}$ 使 $B_1 \oplus B_2 \simeq F(A)$，且可选 B_2 使 F 诱导的 $F_*: \mathrm{End}_{\mathscr{A}} A \to \mathrm{End}_{\mathscr{B}} F(A)$ 为满态射。在此情况下，可以证明必有 Abel 群正合列

$$K_1(\mathscr{A}) \xrightarrow{F_1} K_1(\mathscr{B}) \xrightarrow{\delta} K_0(F) \xrightarrow{\varphi} K_0(\mathscr{A}) \xrightarrow{F_0} K_0(\mathscr{B}) \tag{4}$$

其中连接同态 δ 的定义如下：注意若 $B_1 \in \mathscr{B}, \beta_1 \in \mathrm{Aut} B_1$，则 $K_1(\mathscr{B})$ 中的

$$[B_1, \beta_1] = [B_1 \oplus B_2, \beta_1 \oplus I_{B_2}]$$

可由 $[F(A), \beta]$ 代替，其中 $\beta \in \mathrm{Aut}F(A)$. 于是，对上述满态射 F_*，β 可提升为 A 自态射(记为 α). 定义

$$\delta([F(A), \beta]) = [A, A, \alpha]$$

可验知 δ 为完全确定(与 A, α 的选取无关)的群同态。

取 $\mathscr{A}=\text{f. g. }P_R\mathfrak{M}$，$I \lhd R$，$\mathscr{B}=\text{f. g. }P_{R/I}\mathfrak{M}$。令 F 由标准环同态 $R \twoheadrightarrow R/I$ 诱导，则上述的一些要求都是满足的。从而有上述的群正合列(4)，这也正是关于 $K_1(R), K_1(R/I), K_0(R), K_0(R/I)$ 的一个有用的正合列。

§ 17 Descartes 方图与投射模

在 § 13 中我们已提到 Descartes 方图(纤维积,拉回图),对环范畴 Ring 可定义如下。

定义 17.1 设环同态交换图

$$\begin{array}{ccc} R & \xrightarrow{i_2} & R_2 \\ {\scriptstyle i_1}\downarrow & & \downarrow{\scriptstyle j_2} \\ R_1 & \xrightarrow[j_1]{} & S \end{array} \qquad (1)$$

满足:$\forall (r_1, r_2) \in R_1 \times R_2$,若 $j_1(r_1) = j_2(r_2)$,则有惟一的 $r \in R$ 使 $i_l(r) = r_l$,$l = 1, 2$,则称(1)为(环同态的)**Descartes 方图**,又简称为 ***D* 方图**。

该定义有良好的拓扑背景,比如 § 14 中关于拓扑空间 B 上的纤维丛 (E, P, B) 与 (E', P', B) 的纤维积(Whitney 和)

$$E \oplus E' = \{(e, e') \in E \times E' \mid p(e) = p'(e')\} \xrightarrow[p]{} B$$

事实上可看作是拓扑空间范畴 Top 中的 Descartes 方图。又如

例 1 在 Top 中的交换图

$$\begin{array}{ccc} X_1 \cap X_2 & \rightarrowtail & X_2 \\ \downarrow & \ulcorner\!\bullet & \downarrow \\ X_1 & \rightarrowtail & X_1 \cup X_2 \end{array}$$

经反变函子 C:Top→CRing($C(X) = \{f: X \to F$(取定的域,如 ℝ)$\mid f$ 连续$\}$,见 § 14)即得 CRing 中的 Descartes 图(其中的环同态都是满同态)

$$\begin{array}{ccc} C(X_1 \cup X_2) & \longrightarrow & C(X_2) \\ \downarrow & \bullet\!\lrcorner & \downarrow \\ C(X_1) & \longrightarrow & C(X_1 \cap X_2) \end{array}$$

例 2 对 Descartes 图(1)取 $T = \{t\}$ 或 $\{t, t^{-1}\}$,则可得 Descartes 图

$$\begin{array}{ccc} R[T] & \xrightarrow{i_2'} & R_2[T] \\ {\scriptstyle i_1'}\downarrow & & \downarrow{\scriptstyle j_2'} \\ R_1[T] & \xrightarrow[j_1']{} & S[T] \end{array}$$

上面两图在拓扑学及群环的研究中是有用的工具之一。

由定义 17.1 可直接验证

命题 17.1　在 $\mathfrak{R}$ing 中，下述各点等价：

(1) 图(1)为 Descartes 方图；

(2) 有环同态正合列

$$R \xrightarrow[f]{} R_1 \oplus R_2 \xrightarrow[g]{} S$$

其中 $f=(i_1,i_2)=(i_1\oplus i_2)\Delta, g=(j_1,-j_2)=\Delta^-(j_1\oplus j_2), \Delta: R\to R\oplus R$ 使 $\Delta(r)=(r,r), \Delta^-: j_1R_1\oplus j_2R_2\to S$ 使 $\Delta^-(j_1(r_1),j_2(r_2))=j_1(r_1)-j_2(r_2)$；

(3) R 为

$$\begin{array}{ccc} & & R_2 \\ & \lrcorner & \downarrow j_2 \\ R_1 & \xrightarrow[j_1]{} & S \end{array}$$

的拉回图，即 $R\simeq\{(r_1,r_2)\mid r_j\in R_j, j_1(r_1)=j_2(r_2), i_l(r_1,r_2)=r_l\}$。

当 Descartes 图(1)中的 j_1 或 j_2 满时，此图特别有用。

事实上，$S\in {}_S\mathfrak{M}_{R_l}, l=1,2$，且

$$S\underset{j_l}{\otimes}R_l = S\underset{R_l}{\otimes}R_l \simeq SR_l = S\in {}_S\mathfrak{M}, \qquad l=1,2$$

于是当 j_1 或 j_2 满时，可认为有 ${}_S\mathfrak{M}$(恒等)同构

$$I: S\underset{j_1}{\otimes}R_1 \to S\underset{j_2}{\otimes}R_2$$

使 $I(1_S\otimes r_1)=1_S\otimes r_2$，其中 $j_1(r_1)=j_2(r_2), r_1\in R_1, r_2\in R_2$。因此作为 R-模可记

$$R\simeq(R_1,R_2,I),$$

$$R^n\simeq(R_1^n,R_2^n,I_n),\qquad \text{其中 } I_n: S^n\to S^n \text{ 可视为}{}_S\mathfrak{M}\text{ 恒等同构。}$$

于是，$R^n\in \text{f. g. Free}_R\mathfrak{M}$ 可表为 (R_1^n,R_2^n,I_n) 之形。更一般地，若 $P_l\in$ f. g. $\text{P}_{R_l}\mathfrak{M}$ 且有 ${}_S\mathfrak{M}$ 同构

$$h: S\underset{j_1}{\otimes}P_1\to S\underset{j_2}{\otimes}P_2,$$

$$1_s\otimes x_1\mapsto 1_S\otimes x_2,$$

记 $1=1_s$，且

$$(P_1,P_2,h)=\{(x_1,x_2)\in P_1\times P_2\mid h(1\otimes x_1)=1\otimes x_2\}$$

我们现在给出 R 乘 (P_1,P_2,h) 的定义来证明 $(P_1,P_2,h)\in$ f. g. $\text{P}_R\mathfrak{M}$。不失一般地，设 j_2 满，显然 (P_1,P_2,h) 为 $P_1\times P_2=P_1\oplus P_2$ 的 $\mathbb{Z}$-子模(加法 Abel 群的子群)。定义 R 乘运算为

$$r(x_1,x_2)=(i_1(r)x_1,i_2(r)x_2),$$

$$\forall r \in R, x_j \in P_j,\ j = 1,2$$

验证 h 与 R 乘的相容性后，易知$(P_1, P_2, h) \in {}_R\mathfrak{M}$。事实上，由

$$h(1 \underset{R_1}{\otimes} i_1(r)x_1) = h(1 \cdot i_1(r) \otimes x_1) = h(1 \cdot j_1(i_1(r)) \otimes x_1)$$
$$= h(j_1(i_1(r)) \cdot 1 \otimes x_1) = j_1(i_1(r))h(1 \otimes x_1)$$
$$= j_1(i_1(r))(1 \otimes x_2) = j_2(i_2(r))(1 \otimes x_2)$$
$$= 1 \otimes i_2(r)x_2$$

即知 h 与 R 乘是相容的。

再来证(P_1, P_2, h)有直和补$(Q_1, Q_2, k) = \{(y_1, y_2) \in Q_1 \times Q_2 \mid$存在${}_S\mathfrak{M}$同构 $k: S\underset{j_1}{\otimes}Q_1 \to S\underset{j_2}{\otimes}Q_2$ 使 $k(1\otimes y_1) = 1\otimes y_2\}$使

$$(P_1, P_2, h) \oplus (Q_1, Q_2, k) \simeq (P_1 \oplus Q_1, P_2 \oplus Q_2, h \oplus k)$$

同构于某一个$(R_1^m, R_2^m, I_m) \in \text{f. g. Free}_R\mathfrak{M}$ 的直和项，即可知$(P_1, P_2, h) \in \text{f. g. P}_R\mathfrak{M}$，这里的同构 $u = (u_1, u_2): (X_1, X_2, f) \to (Y_1, Y_2, g)$是指有${}_S\mathfrak{M}$ 同构组成的交换图

$$\begin{array}{ccc} S\underset{j_1}{\otimes}X_1 & \xrightarrow{f} & S\underset{j_2}{\otimes}X_2 \\ \downarrow 1\otimes u_1 & & \downarrow 1\otimes u_2 \\ S\underset{j_1}{\otimes}Y_1 & \xrightarrow{g} & S\underset{j_2}{\otimes}Y_2 \end{array}$$

事实上，由 $P_l \in \text{f. g. P}_{R_l}\mathfrak{M}$ 知，可令

$$P_l \oplus N_l = R_l^{n_l}, \qquad l = 1,2$$

取 $Q_1 = N_1 \oplus R_1^{n_2}$，$Q_2 = N_2 \oplus R_2^{n_1}$，$n = n_1 + n_2$，即得

$$P_l \oplus Q_l = R_l^n, \qquad l = 1,2$$

为找 k，注意

$$S \underset{j_1}{\otimes} Q_1 \simeq S \underset{j_1}{\otimes} (N_1 \oplus R_1^{n_2}) \simeq S \underset{j_1}{\otimes} N_1 \oplus (S \underset{j_1}{\otimes} R_1)^{n_2}$$
$$\simeq S \underset{j_1}{\otimes} N_1 \oplus S^{n_2} \simeq S \underset{j_1}{\otimes} N_1 \oplus (S \underset{j_2}{\otimes} R_2)^{n_2}$$
$$\simeq S \underset{j_1}{\otimes} N_1 \oplus S \underset{j_2}{\otimes} R_2^{n_2} \simeq S \underset{j_1}{\otimes} N_1 \oplus S \underset{j_2}{\otimes} (P_2 \oplus N_2)$$
$$\simeq S \underset{j_1}{\otimes} N_1 \oplus S \underset{j_2}{\otimes} P_2 \oplus S \underset{j_2}{\otimes} N_2$$
$$\simeq S \underset{j_1}{\otimes} N_1 \oplus S \underset{j_1}{\otimes} P_1 \oplus S \underset{j_2}{\otimes} N_2$$
$$\simeq S \underset{j_1}{\otimes} (N_1 \oplus P_1) \oplus S \underset{j_2}{\otimes} N_2 \simeq S \underset{j_1}{\otimes} R_1^{n_1} \oplus S \underset{j_2}{\otimes} N_2$$
$$\simeq S^{n_1} \oplus S \underset{j_2}{\otimes} N_2$$

$$\simeq (S \underset{j_2}{\otimes} R_2)^{n_1} \oplus S \underset{j_2}{\otimes} N_2$$

$$\simeq S \underset{j_2}{\otimes} (N_2 \oplus R_2^{n_1}) \simeq S \underset{j_2}{\otimes} Q_2$$

由上述同构的合成即得${}_S\mathfrak{M}$ 同构

$$k: S \underset{j_1}{\otimes} Q_1 \to S \underset{j_2}{\otimes} Q_2$$

使 $k(1\otimes y_1)=1\otimes y_2, y_l\in Q_l, l=1,2$，于是得$(Q_1,Q_2,k)$。由此即得${}_R\mathfrak{M}$ 同构

$$(P_1,P_2,h)\oplus(Q_1,Q_2,k)\simeq(P_1\oplus Q_1,$$
$$P_2\oplus Q_2, h\oplus k) = (R_1^n, R_2^n, h\oplus k)$$

(至此尚不能断定右端为 f. g. $\mathrm{Free}_R\mathfrak{M}$！ 因为 $h\oplus k$ 未必对应 I_n)。

但注意 $P_l\oplus Q_l = R_l^n, l=1,2$，且

$$S\underset{j_1}{\otimes} R_1^n \simeq S^n \simeq S\underset{j_2}{\otimes} R_2^n$$

上述的${}_S\mathfrak{M}$ 同构 $h\oplus k$ 可视为 $A\in \mathrm{GL}_n(S)$. 因此有${}_R\mathfrak{M}$ 同构

$$(P_1,P_2,h)\oplus(Q_1,Q_2,k)\simeq(R_1^n,R_2^n,A)$$

由此又得${}_R\mathfrak{M}$ 同构(且(P_1,P_2,h)同构于右端的直和项)：

$$(R_1^n,R_2^n,A)\oplus(R_1^n,R_2^n,A^{-1})\simeq(R_1^{2n},R_2^{2n},A\oplus A^{-1})$$

下面只需证明有${}_R\mathfrak{M}$ 同构

$$(R_1^{2n},R_2^{2n},I_{2n})\to(R_1^{2n},R_2^{2n},A\oplus A^{-1})$$

即知$(P_1,P_2,h)\in$ f. g. $\mathrm{P}_R\mathfrak{M}$。

事实上，由引理 5.5 已知 $A\oplus A^{-1}\in \mathrm{E}_{2n}(S)$。由 $j_2: R_2\to S$ 为环的满同态知，必有群的满同态

$$\tilde{j}_2: \mathrm{E}_{2n}(R_2)\to \mathrm{E}_{2n}(S)$$

$$e_{ij}^{x} \longmapsto e_{ij}^{j_2(x)}, \qquad \forall x\in R_2$$

(注意，一般地，j_2 诱导的 $\mathrm{GL}_{2n}(R_2)\to\mathrm{GL}_{2n}(S)$未必为满同态)。即有 $B\in \mathrm{E}_{2n}(R_2)$使 $\tilde{j}_2(B)=A\oplus A^{-1}$。于是有${}_R\mathfrak{M}$ 同构

$$(I,B):(R_1^{2n},R_2^{2n},I_{2n})\to(R_1^{2n},R_2^{2n},A\oplus A^{-1})$$

即有${}_S\mathfrak{M}$ 同构组成的交换图

$$\begin{array}{ccc} S^{2n}\simeq S\underset{j_1}{\otimes}R_1^{2n} & \xrightarrow{I_{2n}} & S\underset{j_2}{\otimes}R_2^{2n}\simeq S^{2n} \\ 1\otimes I\downarrow & & \downarrow 1\otimes B \\ S^{2n}\simeq S\underset{i_1}{\otimes}R_1^{2n} & \xrightarrow[A\oplus A^{-1}]{} & S\underset{j_2}{\otimes}R_2^{2n} \end{array}$$

由此即得下述命题。

命题 17.2 设(1)为 Descartes 方图且 j_1 或 j_2 为满同态，则

(1) $\forall F\simeq R^n\in \text{f. g. Free}_R\mathfrak{M}, F\simeq(R_1^n, R_2^n, I_n)$；

(2) $\forall P_l\in \text{f. g. P}_{R_l}\mathfrak{M}, l=1,2$，在有${}_S\mathfrak{M}$ 同构

$$h: S\underset{j_1}{\otimes} P_1 \to S\underset{j_2}{\otimes} P_2$$

使 $h(1\otimes x_1)=1\otimes x_2$, $\forall x_l\in R_l$，时，$(P_1, P_2, h)\in \text{f. g. P}_R\mathfrak{M}$。

至此，自然要问：$\forall P\in \text{f. g. P}_R\mathfrak{M}$ 是否必有 $P_l\in \text{f. g. P}_{R_l}\mathfrak{M}$ 与 h 使有${}_R\mathfrak{M}$ 同构 $P\simeq(P_1, P_2, h)$？下述命题肯定地回答了这个问题。

命题 17.3 设(1)为 Descartes 方图且 j_1 或 j_2 为满同态，则对任意的 $P\in \text{f. g. P}_R\mathfrak{M}$，必有 $P_l\in \text{f. g. P}_{R_l}\mathfrak{M}$ 与 h 使有${}_R\mathfrak{M}$ 同构 $P\simeq(P_1, P_2, h)$。

证 取 $P_l=R_l\underset{i_l}{\otimes}P, l=1,2$. 由

$$\begin{aligned} S\underset{j_1}{\otimes} P_1 &= S\underset{j_1}{\otimes}(R_1\underset{i_1}{\otimes} P) \\ &\simeq S\underset{j_1 i_1}{\otimes} P = S\underset{j_2 i_2}{\otimes} P \\ &\simeq S\underset{j_2}{\otimes}(R_2\underset{i_2}{\otimes} P)\simeq S\underset{j_2}{\otimes} P_2 \end{aligned}$$

即得${}_S\mathfrak{M}$ 同构

$$h_P: S\underset{j_1}{\otimes} P_1 \to S\underset{j_2}{\otimes} P_2$$

定义

$$\begin{aligned} f_P: P &\to (P_1, P_2, h_p) \\ x &\mapsto (1_{R_1}\otimes x, 1_{R_2}\otimes x) \end{aligned}$$

容易看出 $h_P(1_S\otimes(1_{R_1}\otimes x))=1_S\otimes(1_{R_2}\otimes x)$ 且 f_P 为加群同态。又

$$\begin{aligned} f_P(rx) &= (1_{R_1}\otimes rx, 1_{R_2}\otimes rx) = (i_1(r)\otimes x, i_2(r)\otimes x) \\ &= r(1_{R_1}\otimes x, 1_{R_p}\otimes x) = rf_P(x), \qquad \forall r\in R, x\in P \end{aligned}$$

因此 f_P 为${}_R\mathfrak{M}$ 同态。下面再证 f_P 为${}_R\mathfrak{M}$ 同构。

在${}_R\mathfrak{M}$ 中任取同构 $\alpha: P\to P'$，仿上，有同态 $f_{P'}: P'\to(P'_1, P'_2, h_{P'})$，因此有交换图

$$\begin{array}{ccc} P & \xrightarrow{f_P} & (P_1, P_2, h_p) \\ \alpha\ \downarrow\simeq & & \simeq\downarrow(1\otimes\alpha, 1\otimes\alpha) \\ P' & \xrightarrow[f_{P'}]{} & (P'_1, P'_2, h_{p'}) \end{array}$$

于是 f_P 为同构 $\Leftrightarrow$ $f_{P'}$ 为同构。由此知，若 $P\oplus Q\simeq R^n$，则 $f_{P\oplus Q}$ 为同构 $\Leftrightarrow$ f_{R^n} 为同构。但由命题 17.2(1)已知 f_{R^n} 为同构，于是 $f_{P\oplus Q}$ 也为同构。另一方面，由下述的${}_R\mathfrak{M}$ 交换图

$$\begin{array}{ccc} P\oplus Q & \xrightarrow{f_P\oplus f_Q} & (P_1,P_2,h_P)\oplus(Q_1,Q_2,h_Q) \\ f_{P\oplus Q}\downarrow\simeq & & \simeq\downarrow \\ ((P\oplus Q)_1,(P\oplus Q)_2,h_{P\oplus Q}) & \xrightarrow{\simeq} & (P_1\oplus Q_1,\ P_2\oplus Q_2,h_P\oplus h_Q) \end{array}$$

又知 $f_P\oplus f_Q$ 为同构，于是，f_P 为${}_R\mathfrak{M}$ 同构。 □

再来证明命题 17.3 中的 P_1,P_2，在同构意义下是惟一的。即

命题 17.4　设(1)为 Descartes 方图且 j_1 或 j_2 为满同态且 $P\simeq(P_1,P_2,h)$ 为${}_R\mathfrak{M}$ 同构. 则有${}_{R_l}\mathfrak{M}$ 同构

$$P_l\simeq R_l\underset{i_l}{\otimes}P,\qquad l=1,2$$

(因此可记 $P=(P_1,P_2,h)$)。

证　用$\otimes$的泛性质，先定义

$\varphi:R_1\times P\to P_1$

$$(r_1,(x_1,x_2))\mapsto r_1x_1,\qquad \forall r_1\in R,x_l\in P_l,\qquad l=1,2$$

由 $R_1\in{}_{R_1}\mathfrak{M}_R$ 可看出 φ 为 R-双加平衡映射(参见[佟文廷,1998])。于是由$\otimes$的泛性质知，必有${}_{R_1}\mathfrak{M}$ 同态 $g_{P_1}:R_1\underset{i_1}{\otimes}P\to P_1$ 使

$$g_{P_1}(\Sigma r_{1j}\otimes(x_{1_j},x_{2_j}))=\Sigma r_{1j}x_{1_j}$$

容易看出，当 $P=R^n\simeq(R_1^n,R_2^n,I_n)$ 时 g_{R^n} 为${}_{R_1}\mathfrak{M}$ 同构。再仿命题 17.3 之证，令$(\alpha,\beta):P\to P'$为${}_R\mathfrak{M}$ 同构，其中 $P'=(P_1',P_2',h')$。由交换图

$$\begin{array}{ccc} R_1\underset{i_1}{\otimes}P & \xrightarrow{g_{P_1}} & P_1 \\ 1\otimes(\alpha,\beta)\ \downarrow\simeq & & \simeq\downarrow\ \alpha \\ R_1\underset{i_1}{\otimes}P' & \xrightarrow[g_{P_1'}]{} & P_1' \end{array}$$

知，g_{P_1} 为${}_{R_1}\mathfrak{M}$ 同构 $\Leftrightarrow$ $g_{P_1'}$ 为${}_{R_1}\mathfrak{M}$ 同构。

取 $Q=(P_1\oplus P_1',P_2\oplus P_2',h\oplus h')$，又由交换图

$$\begin{array}{ccc} (R_1\underset{i_1}{\otimes}P)\oplus(R_1\underset{i_1}{\otimes}P') & \xrightarrow{g_{P_1}\oplus g_{P'_1}} & P_1\oplus P_1' \\ \downarrow\simeq & & \uparrow g_{Q_1}=g_{P_1\oplus P_1'} \\ R_1\underset{i_1}{\otimes}(P\oplus P') & \xrightarrow{\simeq} & R_1\underset{i_1}{\otimes}Q_1 \end{array}$$

知，$g_{P_1\oplus P'_1}$ 为${}_{R_1}\mathfrak{M}$ 同构$\Leftrightarrow$ $g_{P_1}\oplus g_{P_1'}$ 为${}_{R_1}\mathfrak{M}$ 同构。于是再由 $P\in$ f. g. $P_R\mathfrak{M}$ 及 $g_{R_1^n}$ 为${}_{R_1}\mathfrak{M}$ 同构即知 g_{P_1} 为${}_{R_1}\mathfrak{M}$ 同构。同理知有${}_{R_2}\mathfrak{M}$ 同构 $R_2\underset{i_2}{\otimes}P\to P_2$。 □

再来证明：在命题 17.3 的分解 $P\simeq(P_1,P_2,h)$ 中可将${}_R\mathfrak{M}$ 同构分解

为${}_{R_1}\mathfrak{M}$与${}_{R_2}\mathfrak{M}$的同构，即

命题 17.5 设(1)为 Descartes 方图且 j_1 或 j_2 为满同态。若 $P=(P_1, P_2, h)$，$P'=(P'_1 P'_2, k)$，则对任意的${}_R\mathfrak{M}$ 同构 $\alpha: P\to P'$ 必有${}_{R_l}\mathfrak{M}$ 同构 $\beta_l: P_l \to P'_l$，$l=1,2$，使 $\alpha=(\beta_1, \beta_2)$。

证 用命题 17.4 证明中的记号，由交换图

$$\begin{array}{ccc} R_l \underset{i_l}{\otimes} P & \xrightarrow[\simeq]{g_{P_l}} & P_l \\ 1\otimes\alpha \downarrow \simeq & & \downarrow \beta_l \\ R_l \underset{i_l}{\otimes} P' & \xrightarrow[g_{P'_l}]{\simeq} & P'_l \end{array}$$

可定义${}_{R_l}\mathfrak{M}$ 同构 $\beta_l = g_{P'_l}(1\otimes\alpha)g_{P_l}^{-1}$，$l=1,2$。再由交换图

$$\begin{array}{ccccccc} S\underset{j_1}{\otimes}P_1 & \xrightarrow[\simeq]{1\otimes g_{P_1}^{-1}} & S\underset{j_1}{\otimes}R_1\underset{i_1}{\otimes}P & \xrightarrow[\simeq]{1\otimes 1\otimes\alpha} & S\underset{j_1}{\otimes}R_1\underset{i_1}{\otimes}P' & \xrightarrow[\simeq]{1\otimes g_{P'_1}} & S\underset{j_1}{\otimes}P'_1 \\ h\downarrow\simeq & & & & & & k\downarrow\simeq \\ S\underset{j_2}{\otimes}P_2 & \xrightarrow[\simeq]{1\otimes g_{P_2}^{-1}} & S\underset{j_2}{\otimes}R_2\underset{i_2}{\otimes}P & \xrightarrow[\simeq]{1\otimes 1\otimes\alpha} & S\underset{j_2}{\otimes}R_2\underset{i_2}{\otimes}P' & \xrightarrow[\simeq]{1\otimes g_{P'_2}} & S\underset{j_2}{\otimes}P'_2 \end{array}$$

即知$(\beta_1, \beta_2): P\to P'$为${}_R\mathfrak{M}$ 同构且 $\alpha=(\beta_1,\beta_2)$。 □

上述的命题合起来，完全解决了 Descartes 方图(1)中当 j_1 或 j_2 为满同态时 f. g. $\mathrm{P}_R\mathfrak{M}$ 与 f. g. $\mathrm{P}_{R_l}\mathfrak{M}$，$l=1,2$，之间的对应关系。即在同构意义下可看成有包含函子

$$i: \text{f. g. } \mathrm{P}_R\mathfrak{M} \to (\text{f. g. } \mathrm{P}_{R_1}\mathfrak{M}, \text{f. g. } \mathrm{P}_{R_2}\mathfrak{M})$$
$$= \text{f. g. } \mathrm{P}_{R_1}\mathfrak{M} \times \text{f. g. } \mathrm{P}_{R_2}\mathfrak{M}$$

因此由上将 $P\in$ f. g. $\mathrm{P}_R\mathfrak{M}$ 记为 $P=(P_1, P_2, h)$。事实上，在同构意义下，并未丢失任何信息。下节将在此基础上导出 K_0，K_1 群的正合列以作今后应用的工具之一。事实上，按 Descartes 方图(1)，以< >记同构类，由上已可得出关于有限生成投射模同构类的"Descartes 方图"：

$$\begin{array}{ccc} \langle \text{f. g. } \mathrm{P}_R\mathfrak{M}\rangle & \xrightarrow{R_2\underset{i_2}{\otimes}-} & \langle \text{f. g. } \mathrm{P}_{R_2}\mathfrak{M}\rangle \\ R_1\underset{i_1}{\otimes}- \downarrow & & \downarrow S\underset{j_2}{\otimes}- \\ \langle \text{f. g. } \mathrm{P}_{R_1}\mathfrak{M}\rangle & \xrightarrow{S\underset{j_1}{\otimes}-} & \langle \text{f. g. } \mathrm{P}_S\mathfrak{M}\rangle \end{array}$$

扩大到稳定同构类[]，由命题 17.1 已预见出应有 Abel 群正合列(比较命题 17.1，事实上，这里的 Δ 为 $K_i\Delta$，Δ^- 为 $K_i\Delta^-$)

$$K_0R \xrightarrow{(K_0i_1\oplus K_0i_2)\Delta} K_0(R_1)\oplus K_0(R_2) \xrightarrow{\Delta^-(K_0j_1\oplus K_0j_2)} K_0(S)$$

$$[P]\longmapsto([P_1],[P_2])$$

再配以自同构,也应有 Abel 群正合列

$$K_1(R) \xrightarrow{(K_1i_1\oplus K_1i_2)\Delta} K_1(R_1)\oplus K_1(R_2) \xrightarrow{\Delta^-(K_1j_1\oplus K_1j_2)} K_1(S)$$

利用这个思路,再配上一个连接同态 $\delta: K_1(S)\to K_0(R)$ 使成一个六项同态列。在下节中再证明此列是正合列,并由此给出有趣的应用。

先来定义 $f_0, f_1, g_0, f_1, \delta$(对照前段,尤其是命题 17.1)使成六项同态列:

$$K_1(R)\xrightarrow[f_1]{} K_1(R_1)\oplus K_1(R_2)\xrightarrow[g_1]{} K_1(S)\xrightarrow[\delta]{} K_0$$
$$(R)\xrightarrow[f_0]{} K_0(R_1)\oplus K_0(R_2)\xrightarrow[g_0]{} K_0(S)$$

① f_0:以

$$\Delta: X\to X\oplus X$$
$$x\mapsto(x,x)$$

记对角同态,定义

$$f_0=(K_0i_1\oplus K_0i_2)\Delta$$

对 $\forall[P]\in K_0(R)$,将 P 表为 $P\simeq(P_1,P_2,h)$,因此 $[P]=[P_1,P_2,h]$,由

$$K_0i_l[P_1,P_2,h]=[R_l\underset{i_l}{\otimes}(P_1,P_2,h)]=[P_l],\qquad l=1,2$$

知

$$f_0([P])=f_0([P_1,P_2,h])=([P_1],[P_2])$$

② f_1:仿①定义

$$f_1=(K_1i_1\oplus K_1i_2)\Delta$$

对 $\forall[P,\alpha]\in K_1(R)$(见§15),由上知有 ${}_R\mathfrak{M}$ 同构

$$\beta: P\simeq(P_1,P_2,h)$$

由 ${}_R\mathfrak{M}$ 中同构组成的交换图

$$\begin{array}{ccc} P & \xrightarrow[\simeq]{\alpha} & P \\ \beta\downarrow\simeq & & \simeq\downarrow\beta \\ (P_1,P_1,h) & \xrightarrow[\beta\alpha\beta^{-1}]{\simeq} & (P_1,P_2,h)\end{array}$$

知 $[P,\alpha]=[(P_1,P_2,h),\beta\alpha\beta^{-1}]$。又由命题 17.5 知,有 ${}_{R_l}\mathfrak{M}$ 同构 $\gamma_l: P_l\to P_l$,使 $\beta\alpha\beta^{-1}=(\gamma_1,\gamma_2)$。于是

$$K_1i_1([P,\alpha])=K_1i_1([(P_1,P_2,h),\beta\alpha\beta^{-1}])$$

$$= K_1 i_1([(P_1, P_2, h), (\gamma_1, \gamma_2)])$$
$$= [R_1 \underset{i_1}{\otimes} (P_1, P_2, h), 1 \otimes (\gamma_1, \gamma_2)] = [P_1, \gamma_1]$$

同理

$$K_1 i_2([P, \alpha]) = [P_2, \gamma_2]$$

于是

$$f_1([P, \alpha]) = f_1([(P_1, P_2, h), (\gamma_1, \gamma_2)]) = ([P_1, \gamma_1], [P_2, \gamma_2])$$

③ g_0：记差同态

$$\Delta^-: X \oplus X \to X,$$
$$(x, y) \mapsto x - y$$

定义

$$g_0 = \Delta^- (K_0 j_1 \oplus K_0 j_2)$$

于是 $\forall [P_l] \in K_0(R_l)$，

$$g_0([P_1], [P_2]) = [S \underset{j_1}{\otimes} P_1] - [S \underset{j_2}{\otimes} P_2]$$

④g_1：仿③定义

$$g_1 = \Delta^- (K_1 j_1 \oplus K_1 j_2)$$

即 $\forall [P_l, \alpha_l] \in K_1(R_l)$，

$$g_1([P_1, \alpha_1], [P_2, \alpha_2]) = [S \underset{j_1}{\otimes} P_1, 1 \otimes \alpha_1] - [S \underset{j_2}{\otimes} P_2, 1 \otimes \alpha_2]$$

⑤ δ：注意由 § 15 知，$K_1(R) \simeq K_1(\text{f. g. Free}_R \mathfrak{M})$ 且 $\forall x \in K_1(S)$，可认为 $x = [S^n, A]$，$A \in GL_n(S)$. 定义 $\delta: K_1(S) \to K_0(R)$ 使

$$\delta([S^n, A]) = [R_1^n, R_2^n, A] - [R^n]$$

先验证 δ 是完全确定的。为此，令 $[S^n, A] = [S^m, B]$，$B \in GL_m(S)$. 在 GL(S) 中可记（见 § 15）

$$BA^{-1} \in \mathscr{R} = E(S)$$

仿命题 17.2 之证，不失一般地，可设 j_2 为满同态，可知必有 $C \in E(R_2)$ 使得 $\tilde{j}_2(C) = BA^{-1}$。取充分大的 r 使 $C \in E_r(R_2)$ 且 $r > m, r > n$，则有同构

$$(I, C): (R_1^r, R_2^r, A \oplus I) \xrightarrow[\simeq]{} (R_1^r, R_2^r, B \oplus I)$$

于是

$$\delta([S^n, A]) = [R_1^n, R_2^n, A] - [R^n] = [R_1^n, R_2^n, A] + [R_1^{r-n}, R_2^{r-n}, I]$$
$$- [R_1^{r-n}, R_2^{r-n}, I] - [R_1^n, R_2^n, I]$$
$$= [R_1^r, R_2^r, A \oplus I] - [R^r] = [R_1^r, R_2^r, B \oplus I] - [R^r]$$
$$= [R_1^m, R_2^m, B] - [R^m] = \delta([S^m, B])$$

即，δ 为完全确定的。

再证 δ 为群同态。事实上，由

$$\begin{aligned}\delta([S^n,A]+[S^{n_1},A_1]) &= \delta[S^{n+n_1},A\oplus A_1]\\ &=[R_1^{n+n_1},R_2^{n+n_1},A\oplus A_1]-[R^{n+n_1}]\\ &=[R_1^n,R_2^n,A]-[R^n]+[R_1^{n_1},R_2^{n_1},A_1]-[R^{n_1}]\\ &=\delta([S^n,A])+\delta([S^{n_1},A_1])\end{aligned}$$

即知。

§18　Descartes 方图导出的 K_i 群正合列及其应用

本节中仍设下图为环的 Descartes 方图。

$$\begin{array}{ccc} R & \xrightarrow{i_2} & R_2 \\ {\scriptstyle i_1}\downarrow & & \downarrow{\scriptstyle j_2} \\ R_1 & \xrightarrow[j_1]{} & S \end{array} \tag{1}$$

下面来证明本节的主要结果（即仿代数拓扑中关于同调的 Mayer-Vietoris 列建立的 K_0，K_1 群的六项正合列），即证明上节末给出的六项同态列为正合列。

定理 18.1　设 Descartes 方图(1)中的 j_1 或 j_2 为满同态。则有 K_0 群，K_1 群的六项正合列（**Mayer-Vietoris 列**）

$$\begin{aligned} &K_1(R)\xrightarrow[f_1]{}K_1(R_1)\oplus K_1(R_2)\xrightarrow[g_1]{}K_1(S)\xrightarrow[\delta]{}K_0(R)\\ &\xrightarrow[f_0]{}K_0(R_1)\oplus K_0(R_2)\xrightarrow[g_0]{}K_0(S)\end{aligned}\tag{2}$$

证　先验证(2)为复形，即 $g_1f_1=0$，$\delta g_1=0$，$f_0\delta=0$，$g_0f_0=0$。

① $g_1f_1([R^n,A])=g_1([R_1^n,i_1A],[R_2^n,i_2A])=[S^n,j_1i_1A]-[S^n,j_2i_2A]=0$，其中 i_lA 表示 i_l 作用于 $A\in GL_n(R)$ 的各元素所得的矩阵，余类推。于是 $g_1f_1=0$。

② $$\begin{aligned}\delta g_1([R_1^n,A_1],[R_2^m,A_2])&=\delta([S^n,j_1A_1]-[S^m,j_2A_2])\\ &=\delta([S^n,j_1A_1])-\delta([S^m,j_2A_2])\\ &=[R_1^n,R_2^n,j_1A_1]-[R^n]-([R_1^m,R_2^m,j_2A_2]\\ &\quad-[R^m])\end{aligned}$$

但由上节命题 17.5 又知

$$(R_1^n, R_2^n, j_1A_1) \xrightarrow[(A_1, I)]{\simeq} (R_1^n, R_2^n, I),$$

$$(R_1^m, R_2^m, I) \xrightarrow[(I, A_2)]{\simeq} (R_1^m, R_2^m, j_2A_2)$$

因此

$$[R_1^n, R_2^n, j_2A_1] = [R^n],$$
$$[R_1^m, R_2^m, j_2A_2] = [R^m]。$$

故 $\delta g_1 = 0$。

③ $f_0\delta([S^n, A]) = f_0([R_1^n, R_2^n, A] - [R^n])$

$= f_0([R_1^n, R_2^n, A]) - f_0([R_1^n, R_2^n, I])$

$= ([R_1^n], [R_2^n]) - ([R_1^n], [R_2^n]) = 0$

因此 $f_0\delta = 0$。

④ $g_0f_0([P_1, P_2, h]) = g_0(([P_1], [P_2]))$

$= [S \underset{j_1}{\otimes} P_1] - [S \underset{j_2}{\otimes} P_2] = 0$（注意 h 为同构）

因此又知 $g_0f_0 = 0$。

再来证(2)正合。即再证：$\mathrm{Ker}g_1 \subseteq \mathrm{Im}f_1$，$\mathrm{Ker}\delta \subseteq \mathrm{Im}g_1$，$\mathrm{Ker}f_0 \subseteq \mathrm{Im}\delta$，$\mathrm{Ker}g_0 \subseteq \mathrm{Im}f_0$。

① $\forall ([R_1^n, A_1], [R_2^m, A_2]) \in \mathrm{Ker}g_1$，必有$[S^n, j_1A_1] = [S^m, j_2A_2]$。于是仿上面 δ 的完全确定性的证明知，在 $\mathrm{GL}(S)$ 中$(j_2A_2)^{-1}j_1A_1 \in \mathrm{E}(S)$。可令 j_2 满，于是必有 $B \in \mathrm{E}(R_2)$使 $j_2B = (j_2A_2)^{-1}j_1A_1$。取充分大的 $r > m, n$ 可使 $B \in \mathrm{E}_r(R_2)$。因此，在 $\mathrm{GL}_r(S)$ 中，$j_1(A_1 \oplus I_{r-n}) = j_2(A_2 \oplus I_{r-m})B$。即有$_R\mathfrak{M}$ 同构

$$(A_1 \oplus I_{r-n}, (A_2 \oplus I_{r-m})B) : (R_1^r, R_2^r, I_r) \to (R_1^r, R_2^r, I_r)$$

于是

$$([R_1^n, A_1], [R_2^m, A_2]) = ([R_1^r, A_1 \oplus I_{r-n}], [R_2^r, A_2 \oplus I_{r-m}])$$
$$= ([R_1^r, A_1 \oplus I_{r-n}], [R_2^r, (A_2 \oplus I_{r-m})B])$$

（注意 $B \in \mathrm{E}_r(R_2) \Rightarrow [R_2^r, B] = 0$）

$$= f_1([(R_1^r, R_2^r, I_r), (A_1 \oplus I_{r-n}, (A_2 \oplus I_{r-m})B)])$$

因此 $\mathrm{Ker}g_1 \subseteq \mathrm{Im}f_1$。

② $\forall [S^n, A] \in \mathrm{Ker}\delta$，必有$[R_1^n, R_2^n, A] = [R^n] \in \mathrm{K}_0(R)$，于是$(R_1^n, R_2^n, A)$稳定同构于 R^n，即有 m 与$_R\mathfrak{M}$ 同构

$$\alpha : (R_1^{n+m}, R_2^{n+m}, A \oplus I_m) \xrightarrow[\simeq]{} (R_1^{n+m}, R_2^{n+m}, I_{n+m})$$

将 α 按命题 17.5 分解，知有 $B_i \in \mathrm{GL}_{n+m}(R_i)$使 $\alpha = (B_1, B_2)$。于是有$_S\mathfrak{M}$ 中

的交换图

$$\begin{array}{ccc} S^{n+m} & \xrightarrow{A\oplus I_m} & S^{n+m} \\ j_1B_1\downarrow & & \downarrow j_2B_2 \\ S^{n+m} & \xrightarrow{I_{n+m}} & S^{n+m} \end{array}$$

由此知，$A\oplus I_m=(j_2B_2)^{-1}j_1B_1$。又由引理 15.1 知$[S^m,I_m]=0$。因此，

$$\begin{aligned} [S^n,A] = [S^{n+m},A\oplus I_m] &= [S^{n+m},(j_2B_2)^{-1}j_1B_1] \\ &= [S^{n+m},j_1B_1]-[S^{n+m},j_2B_2] \\ &= g_1([R_1^{n+m},j_1B_1],[R_2^{n+m},j_2B_2]) \end{aligned}$$

于是 $\mathrm{Ker}\delta\subseteq\mathrm{Im}g$。

③ $\forall[P]-[R^n]\in\mathrm{Ker}f_0$。注意$[P]=[P_1,P_2,h]$且

$$\begin{aligned} f_0([P]-[R^n]) &= f_0([P_1,P_2,h])-f_0([R_1^n,R_2^n,I_n]) \\ &= ([P_1],[P_2])-([R_1^n],[R_2^n]) \end{aligned}$$

于是有$[P_l]=[R_l^n]$，$l=1,2$。即有同构 $\alpha:P_1\oplus R_1^m\to R_1^{n+m}$ 与 $\beta:P_2\oplus R_2^r\to R_2^{n+r}$，不失一般地可令 $r=m$。由此可得$_S\mathfrak{M}$ 同构的交换图

$$\begin{array}{ccccc} (S\otimes_{j_1}P_1)\oplus S^m & \xrightarrow[\simeq]{} & S\otimes_{j_1}(P_1\oplus R_1^m) & \xrightarrow[\simeq]{1\otimes\alpha} & S\otimes_{j_1}R_1^{n+m} \\ \simeq\downarrow h\oplus I_m & & & & \simeq\downarrow h' \\ (S\otimes_{j_2}P_2)\oplus S^m & \xrightarrow[\simeq]{} & S\otimes_{j_2}(P_2\oplus R_2^m) & \xrightarrow[\simeq]{1\otimes\beta} & S\otimes_{j_2}R_2^{n+m} \end{array}$$

因此有

$$(P_1\oplus R_1^m,P_2\oplus R_2^m,h\oplus I_m)\simeq(R_1^{n+m},R_2^{n+m},h')$$

于是由$[R^{n+m}]=[R_1^{n+m},R_2^{n+m},I_{n+m}]=[R_1^n,R_2^n,I_n]+[R_1^m,R_2^m,I_m]$知

$$\begin{aligned} [P_1,P_2,h]-[R^n] &= [P_1\oplus R_1^m,P_2\oplus R_2^m,h\oplus I_m]-[R^{n+m}] \\ &= [R_1^{n+m},R_2^{n+m},h']-[R^{n+m}] \quad (\alpha,\beta\text{ 为同构}) \\ &= \delta([S^{n+m},h'])\in\mathrm{Im}\delta \end{aligned}$$

④ 注意

$$K_0(R_1)\oplus K_0(R_2)=\{([P_1]-[R_1^n],[P_2]-[R_2^m])\},$$

$$\begin{aligned} & g_0([P_1]-[R_1^n],[P_2]-[R_2^m]) \\ &= [S\otimes_{j_1}P_1]-[S^n]-[S\otimes_{j_2}P_2]+[S^m] \end{aligned}$$

于是

$$([P_1]-[R_1^n],[P_2]-[R_2^m])\in\mathrm{Ker}g_0$$

时，必有

$$[(S \underset{j_1}{\otimes} P_1) \oplus S^m] = [(S \underset{j_2}{\otimes} P_2) \oplus S^n]$$

即有 r 使成$_S\mathfrak{M}$同构的交换图

$$\begin{array}{ccc}
(S\underset{j_1}{\otimes}P_1)\oplus S^{m+r} & \xrightarrow{\simeq} & (S\underset{j_2}{\otimes}P_2)\oplus S^{n+r} \\
\simeq\downarrow & & \simeq\downarrow \\
S\underset{j_1}{\otimes}(P_1 \oplus R_1^{m+r}) & \xrightarrow[h]{\simeq} & S\underset{j_2}{\otimes}(P_2\oplus R_2^{n+r})
\end{array}$$

由此知，$[P_1\oplus R_1^{m+r}, P_2\oplus R_2^{n+r}, h]\in \mathrm{K}_0(R)$，且

$$\begin{aligned}
&([P_1]-[R_1^n],[P_2]-[R_2^m]) \\
&= ([P_1 \oplus R_1^{m+r}],[P_2 \oplus R_2^{n+r}]) - ([R_1^{n+m+r}],[R_2^{n+m+r}]) \\
&= f_0([P_1 \oplus R_1^{m+r}, P_2 \oplus R_2^{n+r}, h]) \\
&\quad - f_0([R_1^{n+m+r}, R_2^{n+m+r}, I_{n+m+r}]) \in \mathrm{Im} f_0
\end{aligned}$$

□

注① 当 Descartes 方图(1)中的 j_1, j_2 全为满同态(比如 § 17 例 1)时(因而 i_1, i_2 也都是满同态)。可将定理 18.1 中的正合列向左开拓到 K_2 群，成为一个九项的正合列(见[Milnor，1971]，P. 53)，但 Swan 于二十世纪七十年代初证出：此九项正合列不能再向 K_3 群开拓。

下面，作为定理 18.1 的应用，我们给出著名的 Rim 定理(稍加强一点的形式)，并简单地介绍一下代数数论中关于类数计算方面的一些结果。

取 $\xi=\xi_p=e^{2\pi i/p}$，其中 p 为素数，称$\mathbb{Q}(\xi_p)$为 p 次分圆域。此时，$\mathbb{Z}[\xi]=\mathbb{Z}[\xi_p]$为$\mathbb{Q}(\xi_p)$中的代数整元环(整闭包)，因此$\mathbb{Z}[\xi]$为 Dedekind(整)环。在代数数论中早已知道当$\mathbb{Z}[\xi]\in$ UFD(即$\mathbb{Z}[\xi]$的类数 $h=1$)时，更一般地，若 p 为奇素数，且 $p\nmid h$(h 为$\mathbb{Q}(\xi_p)$即$\mathbb{Z}[\xi_p]$的类数)时，$x^p+y^p=z^p$ 无非零整数解(即 Fermat 大定理对 p 成立)。另一方面，又可证明：二次数域都是某一分圆域的子域($\mathbb{Q}(\sqrt{m})<\mathbb{Q}(\xi_{|d|})$)，其中

$$d = \begin{cases} 4m, & m \equiv 2,3 \pmod 4 \\ m, & m \equiv 1 \pmod 4 \end{cases}$$

为$\mathbb{Q}(\sqrt{m})$的判别式(见[Washington，1982]或[潘承洞，1991])。因此，在代数数论中，分圆域的研究占有重要的地位。注意到 p 阶循环群 $G=\{1,g,\cdots,g^{p-1}\}\simeq\mathbb{Z}_p$ 都与 $\xi=\xi_p$ 生成的乘法群同构，也可用$\mathbb{Z}[\xi]$研究整群环$\mathbb{Z}G$。但需注意$\mathbb{Z}G\not\simeq\mathbb{Z}[\xi]$，事实上，在$\mathbb{Z}[\xi]$中 $1+\xi+\cdots+\xi^{p-1}=0$，但在$\mathbb{Z}G$ 中 $1+g+\cdots+g^{p-1}\neq 0$。

考察 Descartes 方图

$$
\begin{array}{ccc}
\mathbb{Z}G & \xrightarrow{i_2} & \mathbb{Z} \\
i_1 \downarrow & & \downarrow j_2 \\
\mathbb{Z}[\xi] & \xrightarrow{j_1} & \mathbb{Z}_p
\end{array}
\tag{3}
$$

其中 $i_1(g)=\xi, i_2(g)=1, j_1(\xi)=\bar{1}, j_2(n)=\bar{n}$. 由于 $j_2(j_1)$ 为满同态,由定理 18.1 知有群正合列

$$
\cdots \to K_1(\mathbb{Z}[\xi]) \oplus K_1(\mathbb{Z}) \xrightarrow{g_1} K_1(\mathbb{Z}_p)
$$
$$
\xrightarrow{\delta} K_0(\mathbb{Z}G) \xrightarrow{f_0} K_0(\mathbb{Z}[\xi]) \oplus K_0(\mathbb{Z}) \xrightarrow{g_0} K_0(\mathbb{Z}_p) \tag{4}
$$

我们已经知道(见定理 3.4),对交换环 R,

$$K_0(R) \simeq \mathbb{Z} \oplus \widetilde{K}_0(R)$$

在§21 我们将定义整环 R 理想类群 $\mathrm{Cl}(R)$ 与类数 $h_R \equiv h = |\mathrm{Cl}(R)|$,并证明:对 Dedekind 环,理想类群 $\mathrm{Cl}(R) \simeq \widetilde{K}_0(R)$,因此类数 $h = |\mathrm{Cl}(R)| = |\widetilde{K}_0(R)|$。对代数数域($\mathbb{Q}$ 的有限代数扩张)F 中的代数整元环 O_F,一种特殊的 Dedckind 环,还将证明 $|\mathrm{Cl}(O_F)| < \infty$(见§23)。因此 $\widetilde{K}_0(\mathbb{Z}[\xi])$ 为有限群,当然更是挠群。于是由定理 4.10 知 $\mathbb{Z}[\xi]$ 为连通环(事实上,也可由 $\mathbb{Z}[\xi]$ 无非平凡的幂等元知 $\mathbb{Z}[\xi]$ 为连通环)。本节下面的理想类群都是关于 Dedckind 环 R 的,暂时可认为是 $\widetilde{K}_0(R)$。

下面用正合列(4)来证明:$K_0(\mathbb{Z}G) \simeq K_0(\mathbb{Z}[\xi])$(尽管 $\mathbb{Z}G \not\simeq \mathbb{Z}[\xi]$!)从而间接地确定了 $\mathbb{Z}G$ 的连通性。

事实上,在(4)中

$$
\begin{array}{rcl}
g_0|_{K_0(\mathbb{Z})}: K_0(\mathbb{Z}) & \to & K_0(\mathbb{Z}_p) \\
\| & & \| \\
\mathbb{Z} & & \mathbb{Z}
\end{array}
$$

为同构。于是

$$K_0(\mathbb{Z}[\xi]) = \mathrm{Ker} g_0 = \mathrm{Im} f_0 = \mathrm{Im}(K_0 i_1 \oplus K_0 i_2)\Delta = \mathrm{Im} K_0 i_1$$

由此知 $K_0 i_1$ 为满同态。

若能证 $K_1 j_1$ 为满同态,则知 g_1 为满同态。由(4)的正合列即知 $\delta=0$。于是有 ${}_{\mathbb{Z}}\mathfrak{M}$ 正合列(注意 $K_0(\mathbb{Z}) \simeq \mathbb{Z}$)

$$0 \to K_0(\mathbb{Z}G) \to K_0(\mathbb{Z}[\xi]) \oplus \mathbb{Z} \to \mathbb{Z} \to 0 \tag{5}$$

由于代数整数环 $\mathbb{Z}[\xi]$ 的类数有限,即 $\widetilde{K}_0(\mathbb{Z}[\xi]) \simeq \mathrm{Cl}(\mathbb{Z}[\xi])$ 为有限群。因此 $K_0(\mathbb{Z}[\xi]) \in \mathrm{f.g.}\,{}_{\mathbb{Z}}\mathfrak{M}$。但由 $\mathbb{Z} \in \mathrm{Free}_{\mathbb{Z}}\mathfrak{M}$,由(5)知

$$K_0(\mathbb{Z}[\xi]) \oplus \mathbb{Z} \simeq K_0(\mathbb{Z}G) \oplus \mathbb{Z}$$

于是由有限生成 Abel 群结构定理即知 $K_0(\mathbb{Z}G)\simeq K_0(\mathbb{Z}[\xi])$。

下面证明 $K_1 j_1$ 为满同态. 注意

$$K_1 j_1 : K_1(\mathbb{Z}[\xi]) \to K_1(\mathbb{Z}_p) \simeq \mathbb{Z}_p^{\cdot} = \{\overline{1},\overline{2},\cdots,\overline{p-1}\}$$

任取 k 使 $1\leqslant k\leqslant p-1$,来证存在 $u\in\mathbb{Z}[\xi]^{\cdot}$ 使 $j_1(u)=\bar{k}\in\mathbb{Z}_p^{\cdot}$ 即知

$$\begin{pmatrix} u & \\ & I_\infty \end{pmatrix} \mapsto \begin{pmatrix} \bar{k} & \\ & I_\infty \end{pmatrix}$$

从而即知 $K_1 j_1$ 满。为此令

$$u = \frac{\xi^k - 1}{\xi - 1} = 1 + \xi + \cdots + \xi^{k-1} \in \mathbb{Z}[\xi]$$

取 $\eta=\xi^k$ 则有 l 使 $\eta^l=\xi$,于是

$$u \cdot \frac{\eta^l - 1}{\eta - 1} = \frac{\xi^k - 1}{\xi - 1} \cdot \frac{\xi - 1}{\xi^k - 1} = 1$$

因此 $u\in\mathbb{Z}[\xi]^{\cdot}$ 且 $j_1(u)=j_1(1+\xi+\cdots+\xi^{k-1})=\bar{k}$。由此即证出 $K_1 j_1$ 满,从而知道 $K_0(\mathbb{Z}G)\simeq K_0(\mathbb{Z}[\xi])$(作为有限生成 Abel 群)。但由于上面已证 $K_0 i_1$ 为满同态,从而

$$K_0(\mathbb{Z}[\xi]) \simeq K_0(\mathbb{Z}G)/\mathrm{Ker}K_0 i_1$$

于是对同构的有限生成 Abel 群 $K_0(\mathbb{Z}[\xi])$与 $K_0(\mathbb{Z}G)$必有 $\mathrm{Ker}K_0 i_1=0$,即 $K_0 i_1$ 为同构。再注意$\mathbb{Z}[\xi]$的类数 h_p 有限,当 h_p 为不同的素数之积时 $\mathrm{Cl}(\mathbb{Z}[\xi])\simeq\widetilde{K}_0(\mathbb{Z}[\xi])$由 h_p 惟一确定。从而 $K_0(\mathbb{Z}[\xi])$及与此同构的 $K_0(\mathbb{Z}G)$也由 h_p 惟一确定。于是我们得到 1959 年 S. Rim 给出的著名定理的加强形式:

命题 18.1 (Rim 定理) 设 $G=\{1,g,\cdots,g^{p-1}\}$为 p(素数)阶循环群,$\xi=e^{2\pi i/p}$,$i_1:\mathbb{Z}G\to\mathbb{Z}[\xi]$由 $i_1(g)=\xi$ 给出,则

(1) $K_0 i_1:K_0(\mathbb{Z}G)\to K_0\,\mathbb{Z}[\xi]$为群同构;

(2) $\widetilde{K}_0(\mathbb{Z}G)$为挠群(且为有限群),因此$\mathbb{Z}G$ 为连通环;

(3) 当$\mathbb{Z}[\xi]$的类数 h_p 为不同的素数之积时,$K_0(\mathbb{Z}G)$由 h_p 惟一确定。

注② 用注①中提到的结果及以后将要证明的 $K_2(\mathbb{Z}_p)=1$(即有限域的 K_2 群必平凡),注意(4)中的 $\delta=0$(上已证)。可得关于 K_1 群的正合列

$$1 \to K_1(\mathbb{Z}G) \xrightarrow{f_1} K_1(\mathbb{Z}[\xi]) \oplus K_1(\mathbb{Z}) \xrightarrow{g_1} K_1(\mathbb{Z}_p) \to 1$$

又由 §7 知 $K_1(\mathbb{Z}[\xi])\simeq\mathbb{Z}[\xi]^{\cdot}$,由 §6 知 $K_1(\mathbb{Z})\simeq\mathbb{Z}_2\simeq\mathbb{Z}^{\cdot}$,由 §5 知 $K_1(\mathbb{Z}_p)\simeq\mathbb{Z}_{p-1}\simeq\mathbb{Z}_p^{\cdot}$,可以证明 $K_1(\mathbb{Z}G)\simeq(\mathbb{Z}G)^{\cdot}$。但群环$(\mathbb{Z}G)^{\cdot}$的确定仍十分艰难。比为 $p=5$ 时 I. Karpilovsky 的一个未发表的结果为$(\mathbb{Z}G)^{\cdot}=\pm G\oplus\langle g^2+g^3-1\rangle\simeq\pm G\oplus\mathbb{Z}$,有兴趣的读者可参看[Karpilovsky,1983]。事实上,对一般的素数 p 可证:$(\mathbb{Z}G)^{\cdot}$ 可分解为一个 $2p$ 阶有限群$\pm G$ 与一个自

由 Abel 群之直和。这个自由 Abel 群在 $p=3$ 时为平凡的，在 $p>3$ 时有秩 $(p-3)/2$(见[Milnor，1971])。

为了进一步的应用，再介绍一个有用的概念。

定义 18.1　设 R 为 S 的子环，$f:R\to S$ 为包含同态且 $S\in$ f. g. $P_R\mathfrak{M}$，则称下面定义的 K_i 群同态

$$f_i^*: K_i(S)\to K_i(R),\qquad i=0,1,2$$

为 f 诱导的**转移同态**(transfer homomorphsm)。

$i=0$ 时，由 $S\in$ f. g. $P_R\mathfrak{M}$ 知 $\forall P\in$ f. g. $P_S\mathfrak{M}$，$P\in$ f. g. $P_R\mathfrak{M}$(此时记 P 为 ${}_RP$)。定义

$$f_0^*: K_0(S)\to K_0(R)$$
$$[P]\mapsto[{}_RP]$$

$i=1$ 时，$\forall A\in GL_n(S)$，可认为 $A\in \mathrm{Aut}(S^n)$。由 $S\in$ f. g. $P_R\mathfrak{M}$ 知，必有 $Q\in$ f. g. $P_R\mathfrak{M}$ 使 $S\oplus Q\simeq R^r\in$ f. g. $\mathrm{Free}_R\mathfrak{M}$，于是

$$S^n\oplus Q^n\simeq R^{nr}\in \text{f. g. } \mathrm{Free}_R\mathfrak{M},$$
$$A\oplus I_{Q^n}\in \mathrm{Aut}(S^n\oplus Q^n)$$

取 $S^n\oplus Q^n$ 的 R-基 $\alpha_1,\alpha_2,\cdots,\alpha_{nr}$，则可得 $A\oplus I_{Q^n}$ 的表示矩阵 $A_1\in GL_{nr}(R)\subset GL(R)$。若取 $S^n\oplus Q^n$ 的另一 R-基 $\beta_1,\beta_2,\cdots,\beta_m$(可能 $m\neq nr$，因为 R 未必为 IBN 环)，得表示矩阵 $A_2\in GL_m(R)$。可用线性代数方法证出 A_1 与 A_2 只相差 $GL(R)$ 的内自同构因子。即，可认为有 $B\in GL(R)$ 使 $A_1=BA_2B^{-1}$。于是，在 Abel 群 $K_1(R)=GL(R)^{ab}$ 中 $\overline{A}_1=\overline{A}_2$(注意 $\overline{B}\overline{A}_2\overline{B}^{-1}=\overline{B}\,\overline{B}^{-1}\overline{A}_2=\overline{A}_2$)。因此可定义(完全确定的同态)

$$f_1^*: K_1(S)\to K_1(R)$$
$$\overline{A}\mapsto\overline{A}_1$$

$i=2$ 时，注意§12 中已证：取 $E(R)$ 的自由表现 $1\to R_1\to F\to E(R)\to 1$(为区别于环 R 将自由表现中的 R 记为 R_1)，则

$$K_2(R)\simeq H_2(E(R),\mathbb{Z})\simeq(R_1\cap[F,F])/[F,R_1]\text{(Schur 乘子)}$$

$\forall A\in E_n(S)$。由命题 5.1，可令 $m\geqslant 3$ 充分大，使 $A\in E_n(S)\subset[GL_n(S),GL_n(S)]$。仿 $i=1$，给出(不计内自同构因子)惟一对应的 $A_1\in[GL(R),GL(R)]=E(R)$。于是通过 Schur 乘子即给出(完全确定的)同态

$$f_2^*: K_2(S)\to K_2(R)$$

由上已得

引理 18.1　设 R 为 S 的子环(更一般地，R 同构于 S 的一个子环)，f：$R\to S$ 为包含同态且 $S\in$ f. g. $P_R\mathfrak{M}$，则在上面定义的转移同态 $f_i^*: K_i(S)\to$

$K_i(R), i=0,1,2$，都存在。

这里，我们只介绍 K_0 群的转移同态的应用。再证明一条引理。

引理 18.2 设 $\xi=\xi_n$ 为 n 次本原单位根，$n\geqslant 3$，则$\mathbb{Z}[\xi+\xi^{-1}]$为$\mathbb{Z}[\xi]$的子环，且$\mathbb{Z}[\xi]\simeq\mathbb{Z}[\xi+\xi^{-1}]^2\in \text{f. g. Free}_{\mathbb{Z}[\xi+\xi^{-1}]}\mathfrak{M}$。

证 由 $\xi^{-1}=\xi^{n-1}$ 知$\mathbb{Z}[\xi+\xi^{-1}]$为$\mathbb{Z}[\xi]$的子环，因此$\mathbb{Z}[\xi]\in {}_{\mathbb{Z}[\xi+\xi^{-1}]}\mathfrak{M}$。

又 ξ 显然满足方程

$$x^2-(\xi+\xi^{-1})x+1=0$$

因此由 $1=1\cdot 1, \xi=1\cdot\xi, \xi^2=(\xi+\xi^{-1})\cdot\xi+(-1)\cdot 1, \xi^3=\xi^2\cdot\xi=(\xi+\xi^{-1})\xi^2-\xi=(\xi+\xi^{-1})^2\xi-(\xi+\xi^{-1})-\xi=((\xi+\xi^{-1})^2-1)\xi-(\xi+\xi^{-1})\cdot 1$，$\cdots$，即知$\{1,\xi\}$为$\mathbb{Z}[\xi]$作为${}_{\mathbb{Z}[\xi+\xi^{-1}]}\mathfrak{M}$ 的生成系。

注意$\mathbb{Z}[\xi+\xi^{-1}]\subset\mathbb{R}$（事实上$\mathbb{Q}(\xi+\xi^{-1})$为$\mathbb{Q}(\xi)$的最大实域，经常被记为$\mathbb{Q}(\xi)^+$），$\xi\notin\mathbb{R}$。$1,\xi$ 肯定是$\mathbb{Z}[\xi+\xi^{-1}]$线性无关的，因此，$1,\xi$ 即为$\mathbb{Z}[\xi]$作为$\mathbb{Z}[\xi+\xi^{-1}]$—模之基，故$\mathbb{Z}[\xi]\in \text{f. g. Free}_{\mathbb{Z}[\xi+\xi^{-1}]}\mathfrak{M}$。 □

由上述两引理立得有助于分圆域$\mathbb{Q}(\xi)$的代数整元环$\mathbb{Z}[\xi]$与它的最大实子域$\mathbb{Q}(\xi+\xi^{-1})\equiv\mathbb{Q}(\xi)^+$的代数整元环$\mathbb{Z}[\xi+\xi^{-1}]$的类数计算的下述结果。

命题 18.2 设 $\xi=\xi_n$ 为 n 次本原单位根，$n\geqslant 3$，则必有转移同态 f_0^*：$K_0(\mathbb{Z}[\xi])\to K_0(\mathbb{Z}[\xi+\xi^{-1}])$在理想类群 $\text{Cl}(\mathbb{Z}[\xi])$上限制的群同态

$$f^*:\text{Cl}(\mathbb{Z}[\xi])\to\text{Cl}(\mathbb{Z}[\xi+\xi^{-1}])$$

因此，$\mathbb{Z}[\xi]$的类数 $h_n=|\text{Ker}f^*|\cdot|\text{Im}f^*|$。

$h_1(n)\equiv|\text{Ker}f^*|$称为$\mathbb{Z}[\xi]$的**相对类数**(relative class number)或类数 h 的**第一因子**。在类域论(class field theorey)中可证明上述的 f^* 为满同态。因 $h_2(n)\equiv|\text{Im}f^*|=|\text{Cl}(\mathbb{Z}[\xi+\xi^{-1}])|$为$\mathbb{Z}[\xi+\xi^{-1}]$的类数，也被称为$\mathbb{Q}(\xi)^+=\mathbb{Q}(\xi+\xi^{-1})$的类数。因此，近代文献中常将 $h_2(n)$（h_n 的第二因子）记为 h_n^+，而将 $h_1(n)$记为 h_n^-，于是 $h_n=h_n^-h_n^+$。

如众周知，Fermat 大定理的研究早已归结为只需考虑 $n=p$ 为奇素数的情况。当 $p\nmid h_p$（当然包括 $h_p=1$，即$\mathbb{Z}[\xi_p]\in$ UFD 的情况）时（此时称 p 为**正则素数**(regular prime)）$x^p+y^p=z^p$ 无非零整数解。尽管 Fermat 大定理已证出，但目前还不知道是否有无穷多个正则素数（只知非正则素数有无穷多个）。1987 年 J. W. Tanner 与 Jr. S. S. Wagstaff 曾算出在不超过 150000（十五万）的正整数中有 13848 个素数，其中正则素数 8399 个。虽然 E. E. Kummer 早已证出：奇素数 P 为正则素数$\Leftrightarrow$ p 不能整除 Bernoulli 数($B_0=1$，递归地，$(m+1)B_m=-\sum_{k=0}^{m-1}\binom{m+1}{k}B_k$，或由 $t/(e^t-1)=\sum_{n=0}^{\infty}B_n\frac{t^n}{n!}$ 可计

算出一切 B_n）$B_2,B_4,B_6,\cdots,B_{p-3}$ 的分子。可以算出 $B_1=-\frac{1}{2}$，$B_2=\frac{1}{6}$，$B_4=-\frac{1}{30}$，$B_6=\frac{1}{42}$，$B_8=-\frac{1}{30}$，$B_{10}=\frac{5}{66}$，$B_{12}=-\frac{691}{2730}$，$B_{14}=\frac{7}{6}$，$\cdots$，B_{20} 的分子为 261082718496449122051，B_{62} 的分子则为一个 110 位的大数，且可证：$\forall k\geqslant 1, B_{2k+1}=0$，且 $\{B_k\}$ 的非零数符号交错地变化，但由此判定大素数的正则性仍是十分艰难的。通过大量的手算，Kummer 发现，当素数 $p\to+\infty$ 时，h_p^+ 变化不大，但 h_p^- 增大很快（比如 $h_{97}^-=411322824001$）。他猜测：(1) $h_p^-\sim 2p\left(\frac{p}{4\pi^2}\right)^{(p-1)/4}$，当 $p\to+\infty$ 时；(2) $h_p=1\Leftrightarrow p\leqslant 19$. 猜测(1)至今尚未解决。但在 1951 年由 N. C. Ankeny 与 S. Chowla 在[Ankeny, 1951]中得出了很好的结果，他们证明了：

$$\log(h_p^-/2p(p/4\pi^2))^{(p-1)/4})=o(\log p),\qquad 当\ p\to+\infty\ 时,$$

因此，对充分大的 p，h_p^- 是严格递增的。猜测(2)于 1971 年由 K. Uchida 证出（H. L. Montgomery 也独立地证出了(2)）（见[Ribenbaim, 1989]）。

J. M. Masley 于 1972 年在他的博士论文中着手进行且于 1976 年与 H. L. Montgomery 联合发表了下述的重要结果：

若 $n\not\equiv 2 \pmod 4$，则 $h_n=1\Leftrightarrow$（除 $n=1$ 时 $\mathbb{Z}[\xi_n]=\mathbb{Z}$ 的平凡情况外）n 为下 29 个数之一：3，4，5；7，8，9；11，12，13；15，16，17；19，20，21；24，25；27，28；32，33；35，36；40，44，45，48，60，84（见[Ribenboim, 1989]）。

用下面的引理，我们可以得到更完美的结果。

引理 18.3　设 $(s,t)=1$，则 $\mathbb{Q}(\xi_s,\xi_t)=\mathbb{Q}(\xi_{st})$，因此当 $2\nmid s$ 时，

$$\mathbb{Q}(\xi_{2s})=\mathbb{Q}(\xi_s),\ \mathbb{Z}[\xi_{2s}]=\mathbb{Z}[\xi_s],\ h_{2s}=h_s$$

证　由 $\xi_s=(\xi_{st})^t$，$\xi_t=(\xi_{st})^s$ 知 $\mathbb{Q}(\xi_s,\xi_t)\subseteq\mathbb{Q}(\xi_{st})$。又由 $(s,t)=1$ 知有 $u,v\in\mathbb{Z}$ 使 $us+vt=1$。于是

$$\xi_{st}=(\xi_{st})^{us}\cdot(\xi_{st})^{vt}=\xi_t^u\cdot\xi_s^v\in\mathbb{Q}(\xi_s,\xi_t)$$

因此 $\mathbb{Q}(\xi_s,\xi_t)\supseteq\mathbb{Q}(\xi_{st})$，故 $\mathbb{Q}(\xi_s,\xi_t)=\mathbb{Q}(\xi_{st})$。

当 $2\nmid s$ 时 $(s,2)=1$，取 $t=2$，则 $\xi_t=-1\in\mathbb{Z}$，于是 $\mathbb{Q}(\xi_{2s})=\mathbb{Q}(\xi_s)$，$\mathbb{Z}[\xi_{2s}]=\mathbb{Z}[\xi_s]$，$h_{2s}=h_s$。　□

由此引理我们立得（注意 $\mathbb{Z}[\xi_n]$ 都是 Dedekind 环）

命题 18.3　$h_n=1$ 即 $\mathbb{Z}[\xi_n]\in$ UFD(PID) $\Leftrightarrow$ 除平凡情况 $n=1,2$ 外，n 为下述 44 个数之一：3，4，$\cdots$，22；24，25，$\cdots$，28；30；32，33，$\cdots$，36；38；40；42；44，45；48；50；54；60；66；70；84；90。

从命题 18.3 可看出：① $n\leqslant 22$ 时，$h_n=1$，即 $\mathbb{Z}[\xi_n]\in$ PID $\subset$ UFD（可以算出 $h_{23}=3$，因此 $\mathbb{Z}[\xi_{23}]\notin$ UFD）；② $n\leqslant 28$ 且 $n\neq 23$ 时，$h_n=1$；③ $h_{p^n}=1$

$\Leftrightarrow p^n=4,8,16,32;3,9,27;5,25;7;11;13;17;19$。

此外,可以证明(参见[Washington,1982]):$h_m \mid h_{km}$,且查该书中的表(该书按 Euler 函数 $\varphi(n)$,即 ξ_n 的最小多项式(分圆多项式)次数大小,列出 h_n^- 的数值表,表中最大的 n 为 1020,$\varphi(1020)=256$,h_{1020}^- 为一个 44 位的大数)可查出 $1\leqslant\varphi(n)\leqslant256$ 的 h_n^-。可以证明:$p \mid h_p \Leftrightarrow p \mid h_p^-$,因此对正则素数的研究用 h_p^- 已足够。

关于 h_p^+ 知道的较少,但 Kummer 已经知道,在小于 197 的素数中只有 163 使 h_p^+ 为偶数。1969 年 H. Bauer 证出:$p<50$ 时 $h_p^+=1$,因此 $h_p=h_p^-$(见[Milnor,1971])。1964 年曾有人猜测:$p<97$ 时 $h_p^+=1$,但 $h_{97}^+\neq1$。

作为本节的结束,我们列出 h_p^- 的数值表,表中第 2,4 列的数字也表示阶数为该数字的循环群。数字之积也表示上述的 $\mathrm{Ker}f^*$ 为相应阶的循环群之直积。由 Bauer 的上述结果知,当素数 $p<50$ 时,该表第 2 列则表出 $\mathrm{Cl}(\mathbb{Z}[\xi_p])$ 即 $\widetilde{\mathrm{K}}_0(\mathbb{Z}[\xi_p])$ 的结构(参见[日本数学会,1985])。

素数次分圆域的相对类数表($p<100$)

p	$h_p^-=h_p$	p	h_p^-
$\leqslant19$	1	53	4889
23	3	59	3 · 59 · 233
29	2 · 2 · 2	61	41 · 1861
31	9	67	67 · 12739
37	37	71	7 · 7 · 79241
41	11 · 11	73	89 · 134353
43	211	79	5 · 53 · 377911
47	5 · 139	83	3 · 279405653
		89	113 · 118401449
		97	577 · 3457 · 206209

第五章　交换环的 K_0 群分解与类数

由于交换环的 K_0 群对代数几何、代数数论等学科有着十分重要的应用，在本章中我们较深入地介绍交换环的 K_0 群的一些更细致的理论。在§19 中先用可逆 R-模(即秩为 1 的有限生成投射 R-模)的同构类定义在代数几何中有重要应用的 Picard 群，并且用外代数工具证明：在同构意义下，交换环 R 的 Picard 群即 K_0 环(R 为交换环使 $K_0(R)$有环结构)的乘法群的子群，对一些重要的交换环类还证明了 Picard 群的平凡性。在§21 则证明对于整环，其 Picard 群与理想类群是同构的。在§20 中用拓扑空间(环 R 的(素)谱)Spec$R$ 上的连续整(值)函数环 $H_0(R)$给出 $K_0(R)$的群直和分解。对重要的 Dedekind 环，在§22 中证明了 K_0 群四种分解的一致性，且作为应用给出对一类虚二次域类数计算的新方法。在§23 中进一步地证明了代数数域中代数整元环的类数必有限，同时介绍对虚二次域及有理函数域计算类数的一些有用的结果及相关的一些问题。在本章末节(§24)，再次用 Descartes 方图导出的正合列介绍计算类数的一些有用工具与方法。

§19　交换环的 Picard 群及其在 K_0 环乘法群中的嵌入

设 R 为交换环，$M\in$ f. g. $P_R\mathfrak{M}$，$P\in \mathrm{Spec}R$，$g:R\to Q(R/P)\equiv F$ 为标准同态。在§4 中我们已定义了 M 在 P 的局部秩

$$\mathrm{rank}_P(M) \equiv \dim_F F \bigotimes_R M = \mathrm{K}_0(g)([M])$$

在对一切 $P \in \mathrm{Spec}R$，$\mathrm{rank}_P(M) = n$ 为常数时，则记

$$\mathrm{rank}(M) = n$$

称 M 有**常数秩** n。我们在 §4 中还证明了：

(1) $\mathrm{rank}_P(M) = n \Leftrightarrow M_P \simeq R_P^n$（即局部秩＝局部化之后的（自由）秩）；

(2) $P_1, P_2 \in \mathrm{Spec}R$ 且 $P_1 \subset P_2$ 时，$\mathrm{rank}_{P_1}(M) = \mathrm{rank}_{P_2}(M)$，因此 R 为整环或交换局部环时，一切 $M \in \mathrm{f.g.\,P}_R\mathfrak{M}$ 都有常数秩。

现记

$$N^* = \mathrm{Hom}_R(N, R), \qquad \forall N \in {}_R\mathfrak{M}$$

则 $N^* \in {}_R\mathfrak{M}$（R 非交换环时，$N^* \in \mathfrak{M}_R$）称为 N 的**对偶模**(dual module)。由

$$\mathrm{Hom}_R(M \oplus N, R) \simeq \mathrm{Hom}_R(M, R) \oplus \mathrm{Hom}_R(N, R)$$

容易得到

引理 19.1 设 $R \in \mathbb{R}\mathrm{ing}$，$M, N \in {}_R\mathfrak{M}$，则

(1) $(M \oplus N)^* \simeq M^* \oplus N^* \in \mathfrak{M}_R$；

(2) $\forall F \in \mathrm{f.g.\,Free}_R\mathfrak{M}$，$F^* \in \mathrm{f.g.\,Free}\mathfrak{M}_R$；

$\forall M \in \mathrm{f.g.\,P}_R\mathfrak{M}$，$M^* \in \mathrm{f.g.\,P}\mathfrak{M}_R$。

下面再给出局部化与对偶模的关系。

引理 19.2 设 $R \in \mathbb{C}\mathrm{Ring}$，$S \subset R$ 为乘法封闭集，则对 f. g. $\mathrm{P}_R\mathfrak{M}$，$S^{-1} * \simeq * S^{-1}$，即

$$S^{-1}(M^*) \simeq (S^{-1}M)^*, \qquad \forall M \in \mathrm{f.g.\,P}_R\mathfrak{M}$$

因此，$\mathrm{rank}_P(M) = \mathrm{rank}_P(M^*)$ 且

$$(M^*)_P \simeq (M_P)^*, \qquad \forall P \in \mathrm{Spec}R$$

证 由命题 4.2 知，只需证明

$$S^{-1}R \bigotimes_R M^* \simeq \mathrm{Hom}_{S^{-1}R}(S^{-1}M, S^{-1}R)$$

定义

$$\varphi: S^{-1}R \times M^* \to \mathrm{Hom}_{S^{-1}R}(S^{-1}M, S^{-1}R)$$

$$\left(\frac{1}{s}, f\right) \mapsto \frac{1}{s}f, \qquad \forall s \in S, f \in M^*,$$

其中 $\frac{1}{s}f\left(\frac{m}{t}\right) = \frac{f(m)}{st}$，$\forall m \in M, t \in S$。容易看出 φ 为完全确定的 R-双线性映射。因此，由 $\otimes$ 的泛性质知，必有 ${}_R\mathfrak{M}$ 同态 h 使下图为交换图

$$\begin{array}{ccc} S^{-1}R\times M^* & \xrightarrow{\varphi} & \mathrm{Hom}_{S^{-1}R}(S^{-1}M, S^{-1}R) \\ \otimes\downarrow & \nearrow_{h} & \\ S^{-1}R\otimes_R M^* & & \end{array}$$

且 $h(\frac{1}{s}\otimes f)=\frac{1}{s}f$, $\forall s\in S, f\in M^*$。

(1) 先证 h 是单的(注意 $S^{-1}R\underset{R}{\otimes}M^*$ 中的元素都可表为$\frac{1}{s}\otimes f$ 形)。

令$\frac{1}{s}f=0, s\in S, f\in M^*$,则由 φ 的定义可知$\frac{f(m)}{st}=0$,即有 $s_0\in S$ 使得 $s_0f(m)=0$。由 $M\in \mathrm{f.g.}_R\mathfrak{M}$ 知,可令 $M=\langle m_1,\cdots,m_n\rangle$,于是有 $s_j\in S$ 使 $s_jf(m_j)=0$。由此知 $s_1s_2\cdots s_nf(M)=0$,即 $s_1s_2\cdots s_nf=0$。于是

$$\frac{1}{s}\otimes f=\frac{s_1s_2\cdots s_n}{ss_1s_2\cdots s_n}\otimes f=\frac{1}{ss_1s_2\cdots s_n}\otimes s_1s_2\cdots s_nf=0$$

因此 h 是单的。

(2) 再证 h 是满的。

考察下图,其中 $\sigma: R\to S^{-1}R$ 为标准同态,$\beta\in \mathrm{Hom}_{S^{-1}R}(S^{-1}M,S^{-1}R)$。

$$\begin{array}{ccccc} & & M & \xrightarrow{S^{-1}} & S^{-1}M \\ & \swarrow_{f} & \downarrow{\bar\beta} & & \downarrow\beta \\ R & \xrightarrow{\sigma} & \mathrm{Im}\sigma & \xrightarrow[i]{} & S^{-1}R \end{array}$$

$\forall m=\sum_{j=1}^{n}a_jm_j\in M, j\in R$,记 $\beta(\frac{m_j}{1})=\frac{r_j}{s_j}$, $t=s_1s_2\cdots s_n$,则

$$\begin{aligned}\beta(\frac{tm}{1})&=\beta(\frac{t\Sigma a_jm_j}{1})\\&=\Sigma a_jt\beta(\frac{m_j}{1})\\&=\Sigma a_jt\frac{r_j}{s_j}\equiv\frac{r}{s},\ r\in R, s\in S\end{aligned}$$

定义

$$\begin{aligned}\bar\beta: M&\to \mathrm{Im}\sigma\\ m&\mapsto\beta(\frac{tm}{1})=\frac{r}{s}\end{aligned}$$

则 $\bar\beta$ 为 $_R\mathfrak{M}$ 同态。因此,由 $M\in \mathrm{P}_R\mathfrak{M}$ 知,必有 $_R\mathfrak{M}$ 同态 $f: M\to R$ 使得$\frac{f(m)}{1}$

$=\bar{\beta}(m)$, $\forall m \in M$。于是

$$\frac{f(m)}{t} = \frac{1}{t}\beta(\frac{tm}{1}) = \beta(\frac{tm}{t}) = \beta(\frac{m}{1}), \qquad \forall m \in M$$

由此知

$$\beta = \frac{1}{t}f = h(\frac{1}{t} \otimes f), \qquad \forall \beta \in \mathrm{Hom}_{S^{-1}R}(S^{-1}M, S^{-1}R)$$

即 h 是满的。 □

由上面证明中的(1)立得如下推论

推论 19.1 设 $R \in \mathbb{C}\mathrm{Ring}$, $M \in \mathrm{f.g.}_R\mathfrak{M}$,则有单同态 $S^{-1}(M^*) \to (S^{-1}M)^*$。

注① 引理中的条件 $M \in \mathrm{f.g.P}_R\mathfrak{M}$ 可放宽为 $M \in \mathrm{f.p.}_R\mathfrak{M}$(有限表示(相关)$R$-模类),见[Rotman,1979]。

引理 19.3 设 $R \in \mathbb{C}\mathrm{Ring}$,则

(1) $\forall M \in {}_R\mathfrak{M}$,下述三点等价($\mathrm{rank}_P(M)$仍定义为 $\dim F \otimes_R M$):

(i) $M=0$; (ii) $M_P=0$, $\forall P \in \mathrm{Spec}R$; (iii) $M_P=0$, $\forall P \in \mathrm{Max}R$。

(2) $\forall M \in \mathrm{f.g.P}_R\mathfrak{M}$, $M=0 \Leftrightarrow \mathrm{rank}(M)=0$。

证 (1) $\Rightarrow$(2)是显见的(注意 $\forall M \in \mathrm{f.g.P}_R\mathfrak{M}$, $\mathrm{rank}_P(M)=n \Leftrightarrow M_P \simeq R_P^n$)。

(1)中(i)$\Rightarrow$(ii)$\Rightarrow$(iii)是显见的,只需再证(iii)$\Rightarrow$(i)。

设(iii)成立但 $M \neq 0$,则有 $0 \neq m \in M$ 使 $Ann(m)=\{r \in R \mid rm=0\} \subsetneqq R$(因 $1_R \notin Ann(m)$)。于是有 $P \in \mathrm{Max}R$ 使 $P \supset Ann(m)$,但由 $M_P=0$ 知 $\frac{m}{1}=0$ 于是有 $t \in R \setminus P$ 使 $tm=0$,即 $t \in Ann(m)$,这与 $t \notin P \supset Ann(m)$ 矛盾。 □

引理 19.4 设 $R \in \mathbb{C}\mathrm{Ring}$, $M, N \in {}_R\mathfrak{M}$, $P \in \mathrm{Spec}R$,则

(1) $(M \otimes_R N)_P \simeq M_P \otimes_{R_P} N_P$;

(2) $(M \oplus N)_P \simeq M_P \oplus N_P$;

(3) $\mathrm{rank}_P(M \otimes_R N) = \mathrm{rank}_P(M) \cdot \mathrm{rank}_P(N)$, $\forall M, N \in \mathrm{f.g.P}_R\mathfrak{M}$;

(4) $\mathrm{rank}_P(M \oplus N) = \mathrm{rank}_P(M) + \mathrm{rank}_P(N)$。

证 令 $S=R \setminus P$,则 $\forall X \in {}_R\mathfrak{M}$, $X_P = S^{-1}X \simeq S^{-1}R \otimes_R X$。于是有

$$\begin{aligned}(M \otimes_R N)_P &\simeq S^{-1}R \otimes_R (M \otimes_R N) \simeq (S^{-1}R \otimes_R M) \otimes_R N \\ &\simeq S^{-1}M \otimes_R N \simeq S^{-1}M \otimes_{S^{-1}R} S^{-1}R \otimes_R N \\ &\simeq S^{-1}M \otimes_{S^{-1}R} S^{-1}N = M_P \otimes_{R_P} N_P\end{aligned}$$

$$(M\oplus N)_P\simeq S^{-1}R\bigotimes_R(M\oplus N)\simeq S^{-1}R\bigotimes_R M\oplus S^{-1}R\bigotimes_R N$$

$$\simeq S^{-1}M\oplus S^{-1}N=M_P\oplus N_P$$

即(1),(2)成立。

当 $M,N\in$ f. g. $\mathrm{P}_R\mathfrak{M}$ 时,令 $\mathrm{rank}_P(M)=m$,$\mathrm{rank}_P(N)=n$,则由§4 知 $M_P\simeq R_P^m$,$N_P\simeq R_P^n$。于是由(1),(2)知

$$(M\bigotimes_R N)_P\simeq M_P\bigotimes_{R_P}N_P\simeq R_P^m\bigotimes_{R_P}R_P^n\simeq R_P^{nm},$$

$$(M\oplus N)_P\simeq M_P\oplus N_P\simeq R_P^m\oplus R_P^n\simeq R_P^{m+n}$$

由此知

$$\mathrm{rank}_P(M\bigotimes_R N)=mn=\mathrm{rank}_P(M)\cdot\mathrm{rank}_P(N),$$

$$\mathrm{rank}_P(M\oplus N)=m+n=\mathrm{rank}_P(M)+\mathrm{rank}_P(N)$$

即(3),(4)成立。 □

注①　用引理 19.3 中对 $\forall M\in{}_R\mathfrak{M}$,$\mathrm{rank}_PM=\dim F\bigotimes_R M$ 的定义以及上述(1),(2)之证,以 $F\bigotimes_R$- 代 $S^{-1}R\bigotimes_R$- 可证(3),(4)仍成立。

1971 年 W. V. Vasconcelos 曾证出:交换环上有限生成模的满自同态必为自同构(见[McDonald,1984])。对非交换环上的 Noether 模,满自同态也都是同构(见[Berrick,2000])。我们用上述引理可得如下结果。

推论 19.2　设 $R\in\mathcal{C}$Ring,$M,N\in$ f. g. $\mathrm{P}_R\mathfrak{M}$ 且 $\mathrm{rank}_P(M)=\mathrm{rank}_P(N)$,$\forall P\in\mathrm{Max}R$,则任何 R-模满同态 $f:M\twoheadrightarrow N$ 都是同构。

证　由 $N\in\mathrm{P}_R\mathfrak{M}$ 与 f 为满同态知

$$M\simeq\mathrm{Ker}f\oplus N$$

于是由引理 19.4 得(注意 $M\in$ f. g. $\mathrm{P}_R\mathfrak{M}\Rightarrow\mathrm{Ker}f\in$ f. g. $\mathrm{P}_R\mathfrak{M}$)

$$\mathrm{rank}_P(M)=\mathrm{rank}_P(\mathrm{Ker}f)+\mathrm{rank}_P(N)$$

因此有 $\mathrm{rank}_P\mathrm{Ker}f=0$,$\forall P\in\mathrm{Max}R$,由此知,rank Ker$f$ 存在且为 0(注意任一素理想都含于某一个极大理想之中)。从而再由引理 19.3 又知 $\mathrm{Ker}f=0$,即 f 为单同态。故 f 为同构。 □

由以上引理我们可给出定义 Picard 群的基础性定理。

定理 19.1　设 $R\in\mathcal{C}$Ring,$M\in{}_R\mathfrak{M}$,则下述三点等价:

(1) $M\in$ f. g. $\mathrm{P}_R\mathfrak{M}$ 且 $\mathrm{rank}M=1$;

(2) $M^*\bigotimes_R M\simeq R$;

(3) 有 $N\in{}_R\mathfrak{M}$ 使 $N\bigotimes_R M\simeq R$。

在上述条件成立时,使 $N\bigotimes_R M\simeq R$ 的 $N\simeq M^*$。

证 (1)⇒(2):由(1)用引理 19.2 知 $\text{rank}M^*=1$。再由引理 19.4 知 $\text{rank}(M^*\otimes_R M)=1$。令

$$g:M^*\otimes_R M\to R$$
$$f\otimes m\mapsto f(m)$$

($\text{Im}g\equiv\text{tr}(M)$称为 M 的**迹理想**(trace ideal))。由推论 19.2 知为证(2),只需证 g 为满同态。事实上,$\forall P\in\text{Spec}R$,g 诱导出 R_P-模同态

$$g_P:(M^*\otimes_R M)_P\to R_P$$
$$\frac{f\otimes m}{s}\mapsto\frac{f(m)}{s}$$

由引理 19.4 知,在同构意义下可认为这个同态是

$$g_P:M_P^*\otimes_{R_P}M_P\to R_P$$

但 R_P 为局部环,因此 $M_P,M_P^*\in\text{f. g. P}_{R_p}\mathfrak{M}$ 都是有限生成自由的。又 $\text{rank}_P(M)=\text{rank}_P(M^*)=1$。因此,可令 M_P 的基为 m_1。于是 $\forall m\in M_P$,m 可惟一地表为 $m=rm_1$。取 $f\in M_P^*$ 使 $f(m)=r$,则 $f(m_1)=1\in\text{tr}(M_P)$。由此知 g_P 为满同态,$\forall P\in\text{Spec}R$. 由推论 4.1 即知 g 为满同态。

(2)⇒(3):取 $N=M^*$ 即可。

(3)⇒(1):由(3)可令

$$N\otimes_R M\xrightarrow[\simeq]{h_2}R\xrightarrow[\simeq]{h_1}M\otimes N$$

且令 $h_1(1)=\sum_{j=1}^{n}m_j\otimes n_j$,$m_j\in M$,$n_j\in N$。记下图中实线表示的同构之合成为 α(仍为同构)。

$$\begin{array}{ccccc}
 & & M & \xrightarrow[\cong]{} & R\otimes_R M & \xrightarrow[\cong]{h_1\otimes 1} & (M\otimes_R N)\otimes_R M \\
 & \overset{\gamma}{\nearrow} & \downarrow{\scriptstyle\alpha\,\cong} & & & & \downarrow{\scriptstyle\cong} \\
R^n & \xleftarrow[\beta]{} & M & \xleftarrow[\cong]{} & M\otimes_R R & \xleftarrow[\cong]{1\otimes h_2} & M\otimes_R(N\otimes_R M)
\end{array}$$

则容易看出

$$\alpha(m)=\sum_{j=1}^{n}h_2(n_j\otimes m)m_j$$

定义两个 R-模同态

$$\beta:M\to R^n$$
$$m\mapsto(h_2(n_1\otimes m),\cdots,h_2(n_n\otimes m))$$

$$\gamma: R^n \to M$$
$$(r_1, \cdots, r_n) \mapsto r_1 m_1 + \cdots + r_n m_n$$

则有 $\gamma(\beta\alpha) = I_M$。由此知 M 为 R^n 的直和项,即 $M \in \text{f.g.} P_R\mathfrak{M}$。同理知 $N \in \text{f.g.} P_R\mathfrak{M}$。

又,$\forall P \in \text{Spec}R$,由(3)知

$$\text{rank}_P(N) \cdot \text{rank}_P(M) = \text{rank}_P(N \underset{R}{\otimes} M) = \text{rank}_P R = 1$$

因此 $\text{rank}_P M = 1, \forall P \in \text{Spec}R$,即 $\text{rank}M = 1$,即(1)成立。

当上述条件成立时

$$N \simeq R \underset{R}{\otimes} N \simeq (M^* \underset{R}{\otimes} M) \underset{R}{\otimes} N$$
$$= M^* \underset{R}{\otimes} (N \underset{R}{\otimes} M) \simeq M^* \underset{R}{\otimes} R \simeq M^* \qquad \square$$

由定理 19.1 即可定义 Picard 群如下:

定义 19.1 设 $R \in \mathfrak{C}\text{Ring}, M \in {}_R\mathfrak{M}$ 满足定理 19.1 三条件之一,则称 M 为**可逆 R-模**(invertible R-module). 记 $\langle M \rangle$ 为 M 的 R-模同构类,且记

$$\text{Pic}(R) = \{\langle M \rangle \mid M \in \text{f.g.} P_R\mathfrak{M}, \text{rank}M = 1\}$$

在运算

$$\langle M \rangle \langle N \rangle = \langle M \underset{R}{\otimes} N \rangle$$

之下,$\text{Pic}(R)$ 为 Abel 群,称为 R 的 **Picard 群**(显然 $\langle R \rangle = 1, \langle M \rangle^{-1} = \langle M^* \rangle$)。

Picard 群在交换代数与代数几何中都有重要的应用。今后还将证明:对整环(比如 Dedekind 环),Picard 群与理想类群是同构的。

由于同构必为稳定同构,由上述定义已可看出(注意 $R \in \mathfrak{C}\text{Ring}$ 时,$K_0(R)$ 为(交换)环,其乘法由 $[P] \cdot [Q] = [P \underset{R}{\otimes} Q]$ 给出),下述命题是当然成立的。

命题 19.1 设 $R \in \mathfrak{C}\text{Ring}$,则有群同态

$$\text{Pic}(R) \to (K_0(R))^{\cdot}$$
$$\langle M \rangle \mapsto [M]$$

下面我们将证这个同态为单同态,从而可得到一系列有意义的应用,这里需注意 $[M]$(M 的稳定同构类)与 $\langle M \rangle$(M 的同构类)一般地并不相同。但下面将证:对可逆 R-模二者是相同的。即,可逆模的稳定同构与同构是一回事。现在先来简介一下有关外乘法与外代数的一些基本知识,以便于下面的论证。

设 $R \in \mathfrak{C}\text{Ring}, M \in {}_R\mathfrak{M}$,记 $\otimes^p M = M \underset{R}{\otimes} M \underset{R}{\otimes} \cdots \underset{R}{\otimes} M$($p$ 个 M 的张量积,

即 M 的 p 次张量幂),

$$N^p(M)=\langle\{X_1\otimes X_2\otimes\cdots\otimes X_p \mid X_j\in M,\text{但有 } i\neq j \text{ 使 } X_i=X_j\}\rangle<\otimes^p M\in{}_R\mathfrak{M}$$

(有时也简记为 N^pM),称 $\wedge^p M\equiv\otimes^p M/N^p(M)$ 为 M 的 **p 次外乘幂**(exterior power)。约定 $\wedge^0 M=R$, $\wedge^1=M$, $m_1\otimes m_2\otimes\cdots\otimes m_p$ 在 $\wedge^p M$ 中对应的元素(陪集)记为 $m_1\wedge m_2\wedge\cdots\wedge m_p$,称为 $m_1,m_2,\cdots,m_p$ 的**外积**(exterior product)。再记

$$\wedge M=\bigoplus_{p=0}^{\infty}\wedge^p M$$

规定乘法为

$$(m_1\wedge m_2\wedge\cdots\wedge m_p)\wedge(m_{p+1}\wedge m_{p+2}\wedge\cdots\wedge m_{p+q})=m_1\wedge m_2\wedge\cdots\wedge m_p\wedge m_{p+1}\wedge\cdots\wedge m_{p+q}$$

按分配律(R-线性)开拓,则 $\wedge M$ 为 R-代数,称为 M 上的**外代数**(exterior algebra),有时也称为 M 上的 **Grassmann 代数**。可类似地定义乘法$\otimes$,使

$$\otimes M=\bigoplus_{p=0}^{\infty}\otimes^p M$$

也是 R-代数,称为 M 上的**张量代数**(tensor algebra)。容易证明:上述的 $\wedge M$为$\otimes M$的商代数。

注意在外代数 $\wedge M$ 中,记 $m_1,m_2,\cdots$为 M 的任意元素,由

$$(m_1+m_2)\wedge(m_1+m_2)=m_1\wedge m_2+m_2\wedge m_1+m_1\wedge m_1+m_2\wedge m_2$$

(后两项与此式左边显然为 0)可得

$$m_1\wedge m_2=-m_2\wedge m_1$$

又由定义可知外乘有交错性:

$$m_1\wedge m_2\wedge\cdots\wedge m_p=0,\quad \text{当有 } i\neq j \text{ 使 } m_i=m_j \text{ 时} \tag{1$_1$}$$

容易验证外乘有反对称性

$$m_{\sigma(1)}\wedge m_{\sigma(2)}\wedge\cdots\wedge m_{\sigma(p)}=\varepsilon(\sigma)m_1\wedge m_2\wedge\cdots\wedge m_p \tag{1$_2$}$$

其中

$$\varepsilon(\sigma)=\begin{cases}1, & \sigma\in A_p(\text{偶置换集})\\ -1, & \sigma\notin A_p\end{cases}$$

(一般地,交错$\Rightarrow$反对称,但反对称$\not\Rightarrow$交错。当 $\forall\, 0\neq r\in R, r+r\neq 0$ 即 $\mathrm{Ch}R\neq 2$ 时,二者是等价的。$\mathrm{Ch}R=2$ 时,比如$\mathbb{Z}_2$ 中的乘法为双线性的,由 $1\cdot 1=1=-1\neq 0$ 知,此乘法为反对称但不是交错的)。

此外,容易验证:$\forall M,N\in{}_R\mathfrak{M}$,有 R-模同构

$$\wedge^n(M\oplus N)\simeq\bigoplus_{j=0}^{n}\wedge^j M\otimes\wedge^{n-j}N \tag{2}$$

但作为 R-代数的直和项，在 $\wedge(M\oplus N)$ 中

$$\wedge^n(M\oplus N)\simeq\bigoplus_{j=0}^{n}\wedge^j M\stackrel{\wedge}{\otimes}\wedge^{n-j}N,$$

其中 $\stackrel{\wedge}{\otimes}$ 表示 R-代数的反交换张量积。

下面来证明关于外积的几条引理，为后面的定理证明作准备。

引理 19.5 设 $R\in$ CRing, $M\in{}_R\mathfrak{M}$, S 为 R 中的乘法封闭集，则

$$S^{-1}(\wedge_R^p M)\simeq\wedge_{S^{-1}R}^p(S^{-1}M)$$

因此

$$(\wedge_R^p M)_P\simeq\wedge_{R_P}^p M_P,\ \forall P\in\operatorname{Spec}R$$

证 由引理 19.4 知有 R-模同构

$$S^{-1}(\bigotimes_R{}^p M)\xrightarrow[\simeq]{\alpha}\bigotimes_{S^{-1}R}{}^p(S^{-1}M)$$

又显然有

$$\alpha_1\equiv\alpha|_{S^{-1}(N^pM)}:S^{-1}(N^pM)\to N^p(S^{-1}M)$$

且 α_1 为单同态。再由

$$\forall\ \frac{m_1}{s_1}\otimes\cdots\otimes\frac{m_p}{s_p}\in\bigotimes_{S^{-1}R}{}^p(S^{-1}M),$$

$$\frac{m_i}{s_i}=\frac{m_j}{s_j}\Leftrightarrow 有\ t\in S\ 使\ t(s_jm_i-s_im_j)=0\Rightarrow\frac{ts_jm_i}{ts_i}=\frac{ts_im_j}{ts_j}。$$

由此知 α_1 又是满同态，因此为同构。于是由 $S^{-1}R$-模的行正合交换图(注意 S^{-1} 为正合函子)

$$\begin{array}{ccccccccc}
0\to & S^{-1}(N^pM) & \to & S^{-1}(\bigotimes_R{}^pM) & \to & S^{-1}(\wedge_R^pM) & \to 0\\
 & \simeq\downarrow\alpha_1 & & \simeq\downarrow\alpha & & \downarrow\beta & \\
0\to & N^p(S^{-1}M) & \to & \bigotimes_{S^{-1}R}{}^p(S^{-1}M) & \to & \wedge_{S^{-1}R}^p(S^{-1}M) & \to 0
\end{array}$$

可用图追踪法(或用[佟文廷,1998]上的结果)补上 β 使成新交换图。再由 5-引理(图右补上两个 0 到 0 的零同态)即知 β 为同构。 □

引理 19.6 设 $R\in$ CRing。

(1) 设 $M\in$ f. g. ${}_R\mathfrak{M}$, $x_1,x_2,\cdots,x_m$ 为 M 的生成系，则

$$\wedge^n M=0,\qquad\forall n>m$$

且当 $n\leqslant m$ 时，$\wedge^n M$ 由 $\binom{m}{n}$ 个元素 $\{x_{i_1}\wedge\cdots\wedge x_{i_n}\mid 1\leqslant i_1<i_2<\cdots<i_n\leqslant m\}$ 生成。因此 $\wedge^n M\in$ f. g. ${}_R\mathfrak{M}$;

(2)

$$\wedge^n R^m \simeq \begin{cases} R^{\binom{m}{n}} \in \text{f. g. Free}_R\mathfrak{M}, & n \leqslant m \\ 0, & n > m \end{cases}$$

证 (1)$\otimes^n M$ 显然由$\{x_{i_1}\otimes x_{i_2}\otimes\cdots\otimes x_{i_n} \mid 1\leqslant i_1, i_2, \cdots, i_n\leqslant m\}$生成。因此$\wedge^n M=\otimes^n M/N^n(M)$由$\{x_{i_1}\wedge x_{i_2}\wedge\cdots\wedge x_{i_n} \mid 1\leqslant i_1, i_2, \cdots, i_n\leqslant n\}\equiv A$生成. 其中有$i_s\neq i_t$但$x_{i_s}=x_{i_t}$时$x_{i_1}\wedge x_{i_2}\wedge\cdots\wedge x_{i_n}=0$。$n\leqslant m$时将$A$中足码无重复的元素按式$(1)_2$排成足码递增的(注意当$n>m$时$A$中元素足码必有重复的,因此全为0,即$\wedge^n M=0$)即得(1)。

(2) 取$e_1=(1,0,\cdots,0)^T,\cdots,e_m=(0,0,\cdots,1)^T$为$R^m$之标准基(注意CRing$\subset$IBN,$R^m$一切基均含$m$个元)由(1)知,当$n>m$时,$\wedge^n R^m=0$。

当$n=m$时,由(1) 知$e_1\wedge\cdots\wedge e_m$为$\wedge^m R^m$的生成系(元)。又

$$\det: \underbrace{R^m\times\cdots\times R^m}_{m}\rightarrow R$$

为m重R-线性映射。由$\otimes$的泛性质知,有惟一的R-线性映射h(R-模同态)使成交换图

$$\begin{array}{ccc} R^m\times\cdots\times R^m & \longrightarrow & \otimes^m R^m \\ \downarrow \det & \swarrow h & \\ R & & \end{array}$$

由行列式性质(将R^m看作R上的m元列向量集,两列相同的行列式为0)知,$N^m(R^m)\subseteq \text{Ker}h$。因此有$h$诱导的$R$-模同态$\bar{h}: \wedge^m R^m\rightarrow R$. 但$\det(e_1, \cdots, e_m)=1$而$\bar{h}(e_1\wedge\cdots\wedge e_m)=\det(e_1,\cdots,e_m)=1$。由此知$e_1\wedge\cdots\wedge e_m\neq 0$。且对任意的$0\neq r\in R$,

$$re_1\wedge\cdots\wedge e_m\neq 0 \tag{3}$$

因此$n=m$时$\wedge^n R^m\simeq R^{\binom{m}{n}}=R$(以$e_1\wedge\cdots\wedge e_m$为基)。

当$n<m$时,由(1)已知$\{e_{i_1}\wedge\cdots\wedge e_{i_n} \mid 1\leqslant i_1<i_2<\cdots<i_n\leqslant m\}$为$\wedge^n R^m$的生成系(共$\binom{m}{n}$个元素)。为证(2),只需再证,该生成系是$R$-线性无关的。

事实上,反设

$$\Sigma r_{i_1\cdots i_n} e_{i_1}\wedge\cdots\wedge e_{i_n}=0, \qquad 0\neq r_{i_1\cdots i_n}\in R$$

记$\{j_1,\cdots,j_{m-n}\}=\{1,\cdots,m\}\backslash\{i_1,\cdots,i_n\}$。以$e_{j_1}\wedge\cdots\wedge e_{j_{m-n}}$乘上式两端,由$(1)_1$并按$(1)_2$式运算法则重排,则得左边只剩一项的等式

$$\pm r_{i_1\cdots i_n} e_1\wedge\cdots\wedge e_m=0$$

与(3)矛盾。这就证出了(2)。 □

引理 19.7　设 $R\in\mathcal{C}\mathrm{Ring}, M\in \mathrm{f.g.\,P}_R\mathfrak{M}$，则

(1) $\wedge^n M\in \mathrm{f.g.\,P}_R\mathfrak{M}$；

(2) $\forall P\in \mathrm{Spec}R$，记 $\mathrm{rank}_P M=m$，必有

$$\mathrm{rank}_P(\wedge^n M)=\begin{cases}\binom{m}{n}, & m\geqslant n\\ 0, & m<n\end{cases}$$

(3) 当 $\mathrm{rank}M=m$ 时，必有

$$\mathrm{rank}\ \wedge^n M=\begin{cases}\binom{m}{n}, & m\geqslant n\\ 0, & m<n\end{cases}$$

(4) 当 M 为可逆 R-模时，必有 $\wedge^n M=0, \forall n\geqslant 2$。

证　由(2)式，令 $M\oplus N\simeq R^r$，则

$$\wedge^n(M\oplus N)\simeq\bigoplus_{j=0}^{n}(\wedge^j M)\bigotimes_R(\wedge^{n-j}N)=\wedge^n M\oplus\cdots$$

$$\wr|$$

$$\wedge^n R^r\in \mathrm{f.g.\,Free}_R\mathfrak{M}(\text{引理 }19.6(2))$$

由此即得(1)。

由引理 19.5 知，$(\wedge^n M)_P\simeq\wedge^n M_P$。但 $M_P\in \mathrm{f.g.\,Free}_{R_P}\mathfrak{M}$，$m=\mathrm{rank}_P M=\mathrm{rank}M_P$，于是由引理 19.6 即得(2)。

(2)⇒(3)⇒(4)是显见的。 □

再给出一个关键性的引理。

引理 19.8　设 $R\in\mathcal{C}\mathrm{Ring}, M_i, N_j$ 都是可逆 R-模，$i=1,2,\cdots,m, j=1,2,\cdots,n$，且 $M_1\oplus M_2\oplus\cdots\oplus M_m\simeq N_1\oplus N_2\oplus\cdots\oplus N_n$，则

(1) $m=n$；

(2) $M_1\bigotimes_R M_2\bigotimes_R\cdots\bigotimes_R M_m\simeq N_1\bigotimes_R N_2\bigotimes_R\cdots\bigotimes_R N_n$。

证　由定义 19.1 知，可逆模即常数秩为 1 的有限生成投射模。因此

$$\begin{aligned}m&=\mathrm{rank}(M_1\oplus M_2\oplus\cdots\oplus M_m)\\&=\mathrm{rank}(N_1\oplus N_2\oplus\cdots\oplus N_n)=n\end{aligned}$$

即(1)成立。

由引理 19.7(4)知，$\wedge^k M_j=0, \forall k\geqslant 2, j=1,2,\cdots,m$，且

$$\wedge^l(M_2\oplus\cdots\oplus M_m)=0,\qquad \forall l\geqslant m$$

于是由(2)式可得

$$\wedge^m(M_1\oplus\cdots\oplus M_m)\simeq\wedge^m(M_1\oplus(M_2\oplus\cdots\oplus M_m))$$

$$\simeq M_1 \underset{R}{\otimes} \wedge^{m-1}(M_2 \oplus \cdots \oplus M_m)$$

$$\simeq \cdots \simeq M_1 \underset{R}{\otimes} M_2 \underset{R}{\otimes} \cdots \otimes M_m$$

由于已证 $m=n$，同理知

$$\wedge^m(N_1 \oplus \cdots \oplus N_n) = \wedge^m(N_1 \oplus \cdots \oplus N_m)$$

$$\simeq N_1 \underset{R}{\otimes} N_2 \underset{R}{\otimes} \cdots \underset{R}{\otimes} N_m$$

故

$$M_1 \underset{R}{\otimes} M_2 \underset{R}{\otimes} \cdots \underset{R}{\otimes} M_m \simeq N_1 \underset{R}{\otimes} N_2 \underset{R}{\otimes} \cdots \underset{R}{\otimes} N_n$$ □

现在可以证明本节的一个主要结果。

定理 19.2 设 $R\in \mathbb{C}\mathrm{Ring}$，则有嵌入同态(Abel 群单同态)

$$i:\mathrm{Pic}(R) \to (\mathrm{K}_0(R))^{\cdot}$$

$$\langle M\rangle \mapsto [M]$$

证 由命题 19.1 知，只需再证 i 是单的。

事实上，令 $\langle M\rangle,\langle N\rangle \in \mathrm{Pic}(R)$，则 $[M]=[N]$，因此有 $n\in \mathbb{N}$ 使

$$M\oplus R^n \simeq N\oplus R^n$$

于是由引理 19.8 即知

$$M \simeq M \underset{R}{\otimes} R \underset{R}{\otimes} \cdots \underset{R}{\otimes} R \simeq N \underset{R}{\otimes} R \underset{R}{\otimes} \cdots \underset{R}{\otimes} R \simeq N$$

即 $\langle M\rangle=\langle N\rangle$。因此 i 是单的。 □

由此定理可得如下两个推论

推论 19.3 设 $R\in \mathbb{C}\mathrm{Ring}$，则可逆 R-模间的稳定同构即同构。

推论 19.4 设 $R\in \mathbb{C}\mathrm{Ring}$，则

(1) 当 $R\in \mathrm{PSF}$ 时，$\mathrm{Pic}(R)\simeq \mathbb{Z}_2$ 或 1(平凡群)；

(2) 当 R 是(同调)正则的 PSF 环时，

$$\mathrm{Pic}(R[x_1,\cdots,x_n]) \simeq \mathbb{Z}_2 \text{ 或 } 1$$

证 注意 $R\in \mathrm{PSF}\cap \mathbb{C}\mathrm{Ring}$ 时 $\mathrm{K}_0(R)\simeq \mathbb{Z}$，$\mathbb{Z}^{\cdot}=\{\pm 1\}\simeq \mathbb{Z}_2$ 由本定理即得(1)。

注意，对(同调)正则环 R，

$$\mathrm{K}_0(R[x_1,\cdots,x_n]) \simeq \mathrm{K}_0(R)$$

由(1)即得(2)。 □

注② 可以证明：若 R 为左(同调)正则环，$\mathrm{G}_j(R)=\mathrm{K}_j(\mathrm{f.g.}\,{}_R\mathfrak{M})$，则

$$\mathrm{K}_j(R)\simeq \mathrm{G}_j(R) \simeq \mathrm{K}_j(R[x_1,\cdots,R_n])$$

$$\simeq \mathrm{G}_j(R[R_1,\cdots,R_n],\ j=0,1,2,\cdots$$

(见[Lam,1999])。

对(同调)正则整环 R，可证(见[Lam,1999_1])：$R\in \mathrm{UFD}\Leftrightarrow \mathrm{Pic}(R)=1$。

在代数几何中若记仿射代数簇 V 的坐标环为 R,$R\in$ UFD 正好表示着 V 的上维数为 1 的子簇都是 V 与一个超曲面之交.因此 Picard 群与著名的完全交问题也有密切关系。下面我们来证明:对一些概括广的环类,其 Picard 群都是平凡的。

命题 19.2 设 R 为下述环类之一:交换的半局部环,交换的 PF 环,UFD,则 $\mathrm{Pic}(R)=1$(是平凡的)。

证 设 R 为交换半局部环,由定理 4.1 知,有常数秩的有限生成 R-投射模都是自由的,因此可逆 R-模只有一个同构类,故 $\mathrm{Pic}(R)=1$。

若 R 为交换的 PF 环,即一切有限生成投射 R-模都是自由的,此时当然也有 $\mathrm{Pic}(R)=1$。

若 $R\in$ UFD,由于 UFD 必为 Krull 整环(Dedekind 环为 1 维的 Krull 整环),而对 Krull 整环 R,$\mathrm{Pic}(R)<C(R)$(R 的除子类群),对(同调)正则环二者重合)。但对 Krull 整环 R,$R\in \mathrm{UFD}\Leftrightarrow C(R)=1$(见[Matsumura, 1989])。因此 $R\in$ UFD 时 $\mathrm{Pic}(R)=1$。 □

由此命题可知,交换的 Artin 环,交换的半完全环,交换的完全环,PID 上的 n 元多项式环等环类的 Picard 群都是平凡的。但对 Dedekind 环,现在已经知道(由于以后将证 Picard 群与 $\widetilde{K}_0$ 群同构):Picard 群可为任意的 Abel 群。因此 Picard 群的计算仍是非常必要的。事实上,Dedekind 环的类数这一重要的不变量正是其 Picard 群的阶数。此外对交换环 R 可以证明:若 $\mathrm{Pic}(R)$ 的非单位元阶数都不是 n 的因子,则 $R^{n\times n}$ 作为 R-代数的自同构必为内自同构(即可表为 $Q^{-1}PQ$ 形的自同构)。因此 $\mathrm{Pic}(R)=1$ 或无挠时此结论成立。

最后值得着重指出的是:对交换环 R,我们介绍过的或即将介绍的 $K_0(R)$ 的直和分解都是作为 Abel 群的分解,并非是环的分解。因此,一般地,确定 $K_0(R)$ 的乘法群 $K_0(R)^{\cdot}$ 仍是困难的。比如对交换环 R,定理 3.4 给出的 K_0 群的分解

$$K_0(R)\simeq \mathbb{Z}\oplus \widetilde{K}_0(R)$$

只是环 $K_0(R)$ 的加法群的分解。而作为环,$K_0(R)\simeq \mathrm{End}_{\mathbb{Z}}(\mathbb{Z}\oplus\widetilde{K}_0(R))$,但求加群的自同态环一般地并不是件简单的事,因为这种环同构需用分块矩阵来表示,即

$$K_0(R)\simeq \begin{pmatrix}\mathrm{End}_{\mathbb{Z}}\mathbb{Z} & \mathrm{Hom}_{\mathbb{Z}}(\widetilde{K}_0(R),\mathbb{Z})\\ \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z},\widetilde{K}_0(R)) & \mathrm{End}_{\mathbb{Z}}\widetilde{K}_0(R)\end{pmatrix},$$

其中

$$\mathrm{End}_{\mathbb{Z}}\mathbb{Z}\simeq\mathbb{Z},\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z},\widetilde{K}_0(R))\simeq\widetilde{K}_0(R)。$$

§ 20　交换环的 K_0 群关于 H_0 群的分解

设 $R\in\mathfrak{C}$Ring，在 § 4 中对 $M\in$ f. g. $P_R\mathfrak{M}$ 我们已定义了一个秩函数

$$rk_M:\mathrm{Spec}R\to\mathbb{Z}$$
$$P\mapsto \mathrm{rank}_P(M)$$

并对 Spec$R$ 的 Zariski 拓扑（$\{D(r)=\{P\in\mathrm{Spec}R\mid r\notin P\},\ \forall r\in R\}$为其开集基）与 $\mathbb{Z}$ 的离散拓扑，证明了 rk_M 为连续函数（因而也是有界的，因为 Spec$R$ 是紧致的），更一般地，记

$$H_0(R)=\{f:\mathrm{Spec}R\to\mathbb{Z}\mid f\ 连续\}（也可记为\mathbb{Z}^{\mathrm{Spec}R}\ 或\ C(\mathrm{Spec}R)）$$

并规定其运算同函数运算：

$$f+g:(f+g)(P)=f(P)+g(P),$$
$$fg:(fg)(P)=f(P)g(P),\qquad \forall P\in\mathrm{Spec}R,f,g\in H_0(R)$$

容易看出，此时 $H_0(R)\in\mathfrak{C}$Ring，称为 R 的 **H_0 环**（对加法称为 R 的 **H_0 群**）。

设 $\varphi:R\to S$ 为环同态. 定义

$$H_0(\varphi):H_0(R)\to H_0(S)$$
$$g\mapsto g\varphi^*$$

$$\begin{array}{ccc}\mathrm{Spec}R & \xleftarrow{\ \varphi^*\ } & \mathrm{Spec}S\\ & {\scriptstyle g}\searrow \quad \swarrow{\scriptstyle g\varphi^*=H_0(\varphi)(g)} & \\ & \mathbb{Z} & \end{array}$$

其中 $\varphi^*=\mathrm{Spec}(\varphi):\mathrm{Spec}S\to\mathrm{Spec}R$ 使 $\varphi^*(Q)=\varphi^{-1}(Q)$，$\forall Q\in\mathrm{Spec}S$（容易看出 $\varphi^{-1}(Q)\in\mathrm{Spec}R$），则 φ^* 为连续映射。事实上 Spec：$\mathfrak{C}$Ring→Top 为反变函子（对非交换环 Spec$R$ 未必为反变函子。比如 F 为域时取 R 为 $F^{2\times2}$ 中的上三角矩阵环。$S=F^{2\times2}$（单环，$O_s\in\mathrm{Spec}S$），$i:R\to S$ 为包含同态时 $O_R=i^{-1}(O_S)$，但 $O_R\notin\mathrm{Spec}R$，因为

$$A=\begin{pmatrix}0&F\\0&0\end{pmatrix}\lhd R,\qquad A^2=0,但\ A\neq0$$

即 $A\cdot A\subset O_R$，但 $A\not\subset O_R$）。容易验证在 $\mathfrak{C}$Ring 中：

$$\begin{array}{ccc} R & \xrightarrow{\varphi} & S \\ & {\scriptstyle\psi\varphi}\searrow & \swarrow{\scriptstyle\psi} \\ & T & \end{array} \Longrightarrow \begin{array}{ccc} H_0(R) & \xrightarrow{H_0(\varphi)} & H_0(S) \\ & {\scriptstyle H_0(\psi)H_0(\varphi)=H_0(\psi\varphi)}\searrow & \swarrow{\scriptstyle H_0(\psi)} \\ & H_0(T) & \end{array}$$

且 $H_0(I_R)=I_{H_0(R)}$。于是我们已证出下述命题。

命题 20.1　H_0：$\mathcal{C}$Ring→$\mathcal{C}$Ring 为共变函子。

下述命题给出 $K_0(R)$到 $H_0(R)$的环同态。

命题 20.2　设 $R\in\mathcal{C}$Ring，

(1) 有环同态

$$rk: K_0(R)\to H_0(R)$$
$$[M]\mapsto f_M=rk_M$$

(2) 记 $rK_0(R)=\mathrm{Ker}(rk)$，则

$$\begin{aligned} rK_0(R)=&\ \{[M]-[N]\in K_0(R)\mid \mathrm{rank}_P M \\ &=\mathrm{rank}_P N,\ \forall P\in \mathrm{Spec}R\} \\ &=\{[M]-[R^n]\in K_0(R)\mid \mathrm{rank}_P M \\ &=n\geqslant 0,\ \forall P\in\mathrm{Spec}R\} \end{aligned}$$

证　只需证(1)，因为(2)是显见的。

(1) 先证 rk 是完全确定的映射。

设$[M]=[N]$，即有 n 使 $M\oplus R^n\simeq N\oplus R^n$，由此知 $f_M=f_N$，因此 rk 是完全确定的。

再证明 rk 保持加、乘运算的对应(保持单位元对应是显见的)。事实上，

$$rk([M_1]+[M_2])=rk([M_1\oplus M_2])=f_{M_1\oplus M_2}$$

而

$$\begin{aligned} f_{M_1\oplus M_2}(P)=&\ \mathrm{rank}_P(M_1\oplus M_2)=\mathrm{rank}_P(M_1)+\mathrm{rank}_P(M_2) \\ =&\ f_{M_1}(P)+f_{M_2}(P),\qquad \forall P\in\mathrm{Spec}R \end{aligned}$$

即 $f_{M_1\oplus M_2}=f_{M_1}+f_{M_2}$，

$$rk([M_1]+[M_2])=rk([M_1])+rk([M_2]),$$
$$\forall M_1,M_2\in \mathrm{f.g.}\,P_R\mathfrak{M}。$$

同理用$\otimes$得

$$\begin{aligned} rk([M_1][M_2])=&\ rk([M_1\underset{R}{\otimes}M_2])=f_{M_1\otimes M_2}=f_{M_1}\cdot f_{M_2} \\ =&\ rk([M_1])rk([M_2]),\ \forall M_1,M_2\in\mathrm{f.g.}\,P_R\mathfrak{M} \end{aligned}$$ □

下面我们来证明：rk 是函子 K_0，H_0 间的一个自然变换，即

命题 20.3 对 $R\in \mathcal{C}\mathrm{Ring}$，$rk$ 是函子 K_0，H_0 间的自然变换。

证 设 $\varphi:R\to S$ 为环同态，只需证下图为交换图。

$$\begin{array}{ccc} \mathrm{K}_0(R) & \xrightarrow{rk} & \mathrm{H}_0(R) \\ \mathrm{K}_0\varphi \downarrow & & \downarrow \mathrm{H}_0\varphi \\ \mathrm{K}_0(S) & \xrightarrow{rk} & \mathrm{H}_0(S) \end{array}$$

由

$$\mathrm{H}_0\varphi\cdot rk([M]) = \mathrm{H}_0\varphi(f_M) = f_M\varphi^*,$$

其中 $\varphi^*=\mathrm{Spec}(\varphi)$，

$$rk\cdot \mathrm{K}_0\varphi([M]) = rk([S\bigotimes_R M]) = f_{S\bigotimes_R M}, \qquad \forall M\in \mathrm{f.g.}\,\mathrm{P}_R\mathfrak{M}$$

知，只要证明

$$f_{S\bigotimes_R M}(Q) = f_M\varphi^*(Q), \qquad \forall Q\in \mathrm{Spec}S$$

即可。

事实上，

$$\begin{aligned} f_{S\bigotimes_R M}(Q) &= \mathrm{rank}_Q(S\bigotimes_R M) = \mathrm{rank}(S\bigotimes_R M)_Q \\ &= \mathrm{rank}(S_Q\bigotimes_S S\bigotimes_R M) = \mathrm{rank}(S_Q\bigotimes_R M) \end{aligned}$$

记 $P=\varphi^{-1}(Q)$，则

$$\begin{aligned} f_M\varphi^*(Q) &= f_M(P) = \mathrm{rank}_P(M) = \mathrm{rank}M_P \\ &= \mathrm{rank}(R_P\bigotimes_R M) \quad (\text{自由 } R_P\text{- 模的秩}) \\ &\stackrel{!}{=} \mathrm{rank}(S_Q\bigotimes_{R_P} R_P\bigotimes_R M) \\ &= \mathrm{rank}(S_Q\bigotimes_R M) \end{aligned}$$

由此即知欲证成立。 □

注① 命题 20.3 可推广为(见[Swan, 1968])：设 $R,S\in \mathcal{C}\mathrm{Ring}$，$A$ 为 R-代数且 $A\in \mathrm{f.g.}\,\mathrm{P}_R\mathfrak{M}$，$A'$为 S-代数，$A'\in \mathrm{f.g.}\,\mathrm{P}_S\mathfrak{M}$，$h:A\to A'$为环同态 $\varphi:R\to S$ 上的代数同态(即有交换图

$$\begin{array}{ccc} A & \xrightarrow{h} & A' \\ i\uparrow & & \uparrow i' \\ R & \xrightarrow[\varphi]{} & S \end{array}$$

其中 i,i'为分别为 R-代数，S-代数定义中的标准同态)，则 rk 为函子 K_0，H_0 间的自然变换，即有如下的交换图

$$\begin{array}{ccc} K_0(A) & \xrightarrow{rk} & H_0(R) \\ K_0 h \downarrow & & \downarrow H_0\varphi \\ K_0(A') & \xrightarrow[rk]{} & H_0(S) \end{array}$$

注② 若在 $\mathcal{C}$Ring 中 $\varphi: R \twoheadrightarrow S$ 为环满同态，不难证明：

(1) $H_0\varphi$ 为满同态 $\Leftrightarrow$ S 中的任意正交幂等元 $f_1, \cdots, f_n$ 可提升为 R 中的正交幂等元 $e_1, \cdots, e_n$(即 $\varphi(e_j) = f_j, j = 1, 2, \cdots, n$)；

(2) $H_0\varphi$ 为单同态 $\Leftrightarrow$Kerφ 中无非零的幂等元(如 $S \simeq R/\text{rad}R$，φ 为标准环同态，其中 $\text{rad}R = \sqrt{0} = \bigcap_{\forall P \in \text{Spec}R} P$)；

(3) 设 R, S 都为连通环，则 $H_0\varphi$ 为同构；

(4) H_0 保持(环的)有限直积(直和)。

又可证(见[McDonald, 1984])

$$\begin{aligned} rK_0(R) &= \bigcap_{\forall P \in \text{Spec}R} \text{Ker}(K_0(R) \to K_0(R_P)) \\ &= J(K_0(R)) = \text{rad}(K_0(R)) \end{aligned}$$

下面给出 $H_0(R)$ 中任意元素的性质与作用：

命题 20.4 设 $R \in \mathcal{C}$Ring, $f \in H_0(R)$: Spec$R \to \mathbb{Z}$，则有 $n_1, n_2, \cdots, n_r \in \mathbb{Z}$ 使

(1) Im$f = \{n_1, n_2, \cdots, n_r\}$，即 f 的象必为有限集；

(2) $f^{-1}(n_j)$ 为 Spec$R$ 中的闭开集(既是闭集又是开集)，$j = 1, 2, \cdots, r$；

(3) 对某个一 $I_j \lhd R$, $f^{-1}(n_j) = D(I_j)$, $j = 1, 2, \cdots, r$；

(4) $\text{Spec}R = \dot{\bigcup}_{j=1,\cdots,r} D(I_j)$(有限直并)，且 $R = I_1 \oplus \cdots \oplus I_r$；

(5) R 为连通 $\Leftrightarrow$ $r = 1$. $\forall f \in H_0(R)$. 因此 $H_0(R) \simeq \mathbb{Z}$；

(6) 有 R 中的正交幂等元 $e_1, e_2, \cdots, e_r$ 使 $1 = e_1 + e_2 + \cdots + e_r$(称为 **1 对应于 f 的正交幂等元分解**)且 $D(I_j) = D(Re_j)$, $j = 1, 2, \cdots, r$。

证 由 f 的连续性与 $\{n\}$ 为 $\mathbb{Z}$(带离散拓扑)中的闭开集，$\forall n \in \mathbb{Z}$，即知(2)成立。即 $f^{-1}(n)$ 为 Spec$R$ 中的闭开集，注意 Spec$R$ 有开覆盖

$$\text{Spec}R = \bigcup_{n \in Z} f^{-1}(n)$$

但在§4 中我们已知 Spec$R$ 为紧致的拓扑空间。于是 Spec$R$ 有有限的子开覆盖，因此有含开集个数最少的子覆盖，即(1)成立。

记 $I_j = \bigcap_{P \in f^{-1}(n_j)} P$，易见 $I_j \lhd R$ 且 $f^{-1}(n_j) = D(I_j)$，即(3)成立。

$n_i \neq n_j$ 时，$f^{-1}(n_i) \cap f^{-1}(n_j) = \varnothing$，于是(4)成立. 由(4)又知(5)成立。

再由(4)又知 $R=I_1\oplus I_2\oplus\cdots\oplus I_r$(参看引理 4.5 证明中的第一段),于是(6)成立。 □

由此命题与命 4.10 立得如下推论

推论 20.1 设 $R\in$ CRing。

(1) 当 R 连通时,$\mathrm{H}_0(R)\simeq\mathbb{Z}$ 且有限生成投射 R-模都有常数秩。

(2) 当 $\mathrm{K}_0(R)$ 无同构于 $\mathbb{Z}^2$ 的直和项(比如 $\widetilde{\mathrm{K}}_0(R)$ 为挠群)时,$\mathrm{H}_0(R)\simeq\mathbb{Z}$ 且有限生成投射 R-模都有常数秩。

在命题 20.4 的基础上,可给出如下述引理所示的 $\mathrm{H}_0(R)$ 到 $\mathrm{K}_0(R)$ 的环同态。

引理 20.1 设 $R\in$ CRing,则有环同态

$$\theta:\mathrm{H}_0(R)\to\mathrm{K}_0(R)$$

$$f\mapsto\sum_{j=1}^{r}n_j[Re_j]$$

其中 $1=e_1+\cdots+e_r$ 为 1 对应于 f 的正交幂等元分解,$\mathrm{Im}f=\{n_1,n_2,\cdots,n_r\}$。

证 先证明 θ 是完全确定的映射,事实上,注意 r 是由 f 惟一确定的,设 $1=e_1'+\cdots+e_r'$ 也是 1 对应于 f 的正交幂等元分解。由 $1=1\cdot 1$ 知,

$$1=\sum_{i,j=1,\cdots,r}e_ie_j'$$

仍为 1 的正交幂等元分解(上述两分解的公共加细)。于是

$$Re_j=Re_je_1'\oplus\cdots\oplus Re_je'_r$$

从而有

$$[Re_j]=[Re_je_1']+\cdots+[Re_je_r']$$

因此

$$\sum_{j=1}^{r}n_j[Re_j]=\sum_{j=1}^{r}n_j\sum_{i=1}^{r}[Re_je_i']$$

同理知

$$\sum_{i=1}^{r}n_i[Re_i']=\sum_{i=1}^{r}n_i\sum_{j=1}^{r}[Re_je_i']$$

于是

$$\sum_{j=1}^{r}n_j[Re_j]=\sum_{i=1}^{r}n_i[Re_i']$$

即 θ 是完全确定的映射。

仿上,$\forall\, f,g\in\mathrm{H}_0(R)$ 经加细后有公共的正交幂等元分解:$1=e_1+e_2+\cdots+e_n$,使

$$\theta(f)=\sum_{i=1}^{n}n_i[Re_i],$$

$$\theta(g)=\sum_{i=1}^{n}m_i[Re_i]$$

因此有

$$\theta(f+g)=\sum_{i=1}^{n}(n_i+m_i)[Re_i]$$
$$=\sum_{i=1}^{n}n_i[Re_i]+\sum_{i=1}^{n}m_i[Re_i]=\theta(f)+\theta(g)$$

再由 $e_1,e_2,\cdots,e_n$ 的正交幂等性知

$$Re_i\bigotimes_R Re_j=\begin{cases}Re_i, & i=j\\ 0, & i\neq j\end{cases}$$

由此不难看出(用$\otimes$在同构意义下对$\oplus$的分配律):$\theta(fg)=\theta(f)\theta(g)$。又

$$\theta(1)=[R]$$

为 $K_0(R)$的单位元,故 θ 为环同态。 □

现在可证

定理 20.1 设 $R\in$ CRing,则有 Abel 群($\mathbb{Z}$-模)的直和分解

$$K_0(R)\simeq H_0(R)\oplus rK_0(R) \tag{1}$$

证 考察环 $K_0(R)$与 $H_0(R)$的加群,则有$\mathbb{Z}$-模(Abel 群)正合列

$$0\to rK_0(R)\to K_0(R)\xrightarrow[rk]{} H_0(R)$$

$$[M]\longmapsto f_M$$

其中 f_M 使 $f_M(P)=\text{rank}_P M$, $\forall P\in \text{Spec}R$。由此可看出:只需证明 rk 为满可裂的。这归为证明 $rk\theta=I_{H_0(R)}:H_0(R)\to H_0(R)$。即对 $\forall f\in H_0(R)$,设 f 对应的正交幂等元分解为 $1=e_1+e_2+\cdots+e_r$, $f(P)=n_j$, $\forall P\in D(Re_j)$, $j=1,2,\cdots,r$,来证 $rk(\theta(f))=f$,即 $rk(\theta(f)):P\mapsto n_j$, $\forall P\in D(Re_j)$, $j=1,2,\cdots,r$。

事实上,

$$R=\bigoplus_{j=1}^{r}Re_j$$

因此 $Re_j\in$ f. g. $P_R\mathfrak{M}$ 且 $\text{rank}_P(Re_i)\leqslant 1$, $\forall P\in\text{Spec}R$。

更一般地,令 $M=\langle m_1,m_2,\cdots,m_n\rangle\in$ f. g. $P_R\mathfrak{M}$,若 $\text{rank}_P M=0$,即 $M_P=0$,由此知$\frac{m_j}{1}=0\in M_P$。因此有 $s_j\in R\backslash P$ 使 $s_jm_j=0$。取 $s=s_1s_2\cdots s_n$,则 $sM=0$,且 $s\in R\backslash P$,即 $s\in Ann(M)\not\subset P$,于是 $P\in D(Ann(M))$。反过来,若

$P\in D(Ann(M))$，即 $Ann(M)\not\subset P$，则有 $s\in Ann(M)\backslash P$，于是对 $\forall m\in M, t\in R\backslash P$，

$$\frac{m}{t}=\frac{sm}{st}=0$$

即 $M_P=0$，因此 $\mathrm{rank}_P M=0$。由此知

$$\begin{aligned}\{P\in \mathrm{Spec}R \mid \mathrm{rank}_P(Re_1)=0\} &= D(Ann(Re_1))\\ &= D(Re_2+\cdots+Re_r)=\bigcup_{j=2}^{r} D(Re_j)\end{aligned}$$

但

$$\mathrm{Spec}R=\dot{\bigcup_{j=1,2,\cdots,r}} D(Re_j)$$

于是

$$\mathrm{rank}_P(Re_1)=\begin{cases}1, & P\in D(Re_1)\\ 0, & P\notin D(Re_1)\end{cases}$$

同理知

$$\mathrm{rank}_P(Re_j)=\begin{cases}1, & P\in D(Re_j)\\ 0, & P\notin D(Re_j)\end{cases}$$

而

$$\theta(f)=\sum_{j=1}^{r} n_j[Re_j]=[(Re_1)^{n_1}\oplus\cdots\oplus(Re_r)^{n_r}],$$

$$\mathrm{rank}_P((Re_1)^{n_1}\oplus\cdots\oplus(Re_r)^{n_r})=n_j,\qquad \forall P\in D(Re_j)$$

因此

$$rk(\theta(f)):P\mapsto n_j,\qquad \forall P\in D(Re_j),\ j=1,2,\cdots,r$$ □

由上证可得

推论 20.2 设 $R\in$ CRing，$M\in$ f. g. $P_R\mathfrak{M}$，则

$$\{P\mid P\in \mathrm{Spec}R, \mathrm{rank}_P M=0\}=D(Ann(M))$$

其余集 $V(Ann(M))$ 称为 M 的**支撑(支柱)**(support)。

推论 20.3 设 $R\in$ CRing，则

$$H_0(R)=\langle\{f_M\mid M\in \text{f. g. } P_R\mathfrak{M}\}\rangle_{\mathbb{Z}}$$

即作为 Abel 群($\mathbb{Z}$-模)，$H_0(R)$ 可由 $\{f_M \mid M\in$ f. g. $P_R\mathfrak{M}\}$ 生成。因此当 R 为连通环(此时 $\forall M\in$ f. g. $P_R\mathfrak{M}$，M 有常数秩)时有环同构 $H_0(R)\simeq\mathbb{Z}$。

推论 20.4 (1) 引理 20.1 中的环同态 θ 为单同态。因此 $H_0(R)$ 可看成 $K_0(R)$ 的子环；

(2) 命题 20.2 中的环同态 rk 为满同态，因此

$$H_0(R)\simeq K_0(R)/rK_0(R)。$$

下面我们来证明

定理 20.2　设 $R\in$ CRing 为连通环，则

(1) $H_0(R)\simeq\mathbb{Z}$(是 Abel 群同构，也是环同构)；

(2) $\widetilde{K}_0(R)\simeq rK_0(R)$(Abel 群同构)。

因此 Abel 群 $K_0(R)$ 的两种分解：

$$K_0(R)\simeq\mathbb{Z}\oplus\widetilde{K}_0(R)$$

$$K_0(R)\simeq H_0(R)\oplus rK_0(R)\simeq\mathbb{Z}\oplus rK_0(R) \tag{1}$$

是一致的。

证　由推论 20.3 知，只需证(2)，为此考察 $_{\mathbb{Z}}\mathfrak{M}$ 中的行正合交换图

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \widetilde{K}_0(R) & \longrightarrow & K_0(R) & \longrightarrow & \mathbb{Z} & \longrightarrow & 0\\
 & & \downarrow h & & \| & & \downarrow\simeq & & \\
0 & \longrightarrow & rK_0(R) & \longrightarrow & K_0(R) & \longrightarrow & H_0(R) & \longrightarrow & 0
\end{array}$$

由图追踪(或见[佟文廷,1998])知有 $\mathbb{Z}$-模同态 h 使此图仍为交换图。于是由五引理即知 h 为 $\mathbb{Z}$-模(Abel 群)同构。□

我们已经知道交换局部环与整环都是连通环，不可分解 R-模 M(即 M 无非平凡的直和项)的自同态环 $\mathrm{End}_R M$ 也为连通环。事实上可证：M 不可分解$\Leftrightarrow\mathrm{End}_R M$ 的幂等元只有 0,1。建议读者自证或参看[佟文廷,1998]。

由上我们已看出在 Abel 群($\mathbb{Z}$-模)的直和分解式(1)中 θ 为第一标准单同态，rk 为第一标准满同态，记第二个标准满同态为 $\pi: K_0(R)\to rK_0(R)$。则有 $\mathbb{Z}$-模中的可裂正合列

$$0\to H_0(R)\xrightarrow{\theta}K_0(R)\xrightarrow{\pi}rK_0(R)\to 0$$

注意到 $rK_0(R)<K_0(R)$ 知(1)中的第二个标准单同态 $i: rK_0(R)\to K_0(R)$ 即包含映射。于是有 Abel 群的分解

$$K_0(R)=\theta(H_0(R))\oplus rK_0(R)$$

由此知，$\forall[M]\in K_0(R)$ 都有惟一表示式

$$[M]=\theta(f)+[N]-[R^n],\qquad \mathrm{rank}N=n\geqslant 0$$

设对应于 f 的正交幂等元分解为 $1=e_1+e_2+\cdots+e_r$，$f(D(Re_i))=n_i$，则由引理 20.1 知

$$\theta(f)=\sum_{j=1}^{r}n_j[Re_j]$$

于是

$$[N]-[R^n]=[M]-\sum_{j=1}^{r}[(Re_j)^{n_j}]$$

注意 $R^n=(Re_1)^n\oplus\cdots\oplus(Re_r)^n$，则得

$$[N]=[M]+\sum_{j=1}^{r}[(Re_j)^{n-n_j}]$$

因此可取 $n=\max\limits_{1\leqslant j\leqslant r}n_j$，$N=M\oplus(\bigoplus\limits_{j=1}^{r}(Re_j)^{n-n_j})$，故得

命题 20.5 设 $R\in$ CRing，则有 Abel 群的可裂满同态 $\pi: \mathrm{K}_0(R)\twoheadrightarrow r\mathrm{K}_0(R)$ 使

$$\pi([M])=[M]-\theta(f)=[N]-[R^n],\qquad \forall M\in \text{f. g. P}_R\mathfrak{M}$$

其中 N 可表为 $N=M\oplus(\bigoplus\limits_{j=1}^{r}(Re_j)^{n-n_j})$，$n=\max\limits_{1\leqslant j\leqslant r}n_j$，对应于 $f=f_M$ 的正交幂等元分解为 $1=e_1+e_2+\cdots+e_r$。当 R 为连通环时 $N=M$。

§ 21　K_0 群到 Picard 群的行列式映射与整环的 Picard 群

本节中均设 $R\in$ CRing，若 $M\in$ f. g. $\mathrm{P}_R\mathfrak{M}$，$\mathrm{rank}M=m$，由上节知 $[M]-[R^m]\in r\mathrm{K}_0(R)$。又由 § 19 知 $\wedge^m M\in$ f. g. $\mathrm{P}_R\mathfrak{M}$ 且 $\mathrm{rank}\wedge^m M=1$，因此 $\wedge^m M$ 为可逆 R-模。由此知 $\langle\wedge^m M\rangle\in \mathrm{Pic}R$。

若 $[M]-[R^m]=[M_1]-[R^{m_1}]$，$\mathrm{rank}M_1=m_1$，则有

$$[M\oplus R^{m_1}]=[M_1\oplus R^m]$$

于是有 $s\geqslant 0$ 使

$$M\oplus R^{m_1+s}\simeq M_1\oplus R^{m+s}$$

求 $m+m_1+s$ 次外幂，按 § 19 的公式(2)，省写值为 0 的项，则得

$$\begin{aligned}&\wedge^{m+m_1+s}(M\oplus R^{m_1+s})\\&\simeq\wedge^m M\otimes_R\wedge^{m_1+s}R^{m_1+s}\simeq\wedge^m M\otimes_R R\simeq\wedge^m M\end{aligned}$$

同理知

$$\wedge^{m+m_1+s}(M_1\oplus R^{m+s})\simeq\wedge^{m_1}M_1$$

因此 $\wedge^m M\simeq\wedge^{m_1}M_1$，即 $\langle\wedge^m M\rangle=\langle\wedge^{m_1}M_1\rangle$。这样，我们就得到一个完全确定的映射

$$\begin{aligned}\tau: r\mathrm{K}_0(R)&\to \mathrm{Pic}(R)\\ [M]-[R^m]&\mapsto\langle\wedge^m M\rangle\end{aligned}$$

注意，$\forall\langle M'\rangle\in \mathrm{Pic}(R)$，$[M']-[R]\in r\mathrm{K}_0(R)$，$\wedge^1 M'=M'$，于是

$$\tau([M']-[R])=\langle M'\rangle$$

由此知 τ 为满映射。

又设 $M_2\in$ f. g. $\mathrm{P}_R\mathfrak{M}$，$\mathrm{rank}M_2=m_2$，则 $[M_2]-[R^{m_2}]\in r\mathrm{K}_0(R)$ 且

$$\begin{aligned}\tau([M]-[R^m]+[M_2]-[R^{m_2}]) &= \tau([M\oplus M_2]-[R^{m+m_2}])\\ &=\langle\wedge^{m+m_2}(M\oplus M_2)\rangle=\langle\wedge^m M\otimes_R\wedge^{m_2}M_2\rangle\\ &=\langle\wedge^m M\rangle\langle\wedge^{m_2}M_2\rangle\\ &=\tau([M]-[R^m])\tau([M_2]-[R^{m_2}])\end{aligned}$$

于是我们得到

引理 21.1　有 Abel 群的满同态 $\tau: r\mathrm{K}_0(R)\twoheadrightarrow \mathrm{Pic}(R)$ 使

$$\tau([M]-[R^m])=\langle\wedge^m M\rangle$$

将命题 20.5 与此引理合起来，即得

命题 21.1　设 $R\in\mathcal{C}\mathrm{Ring}$，则有 Abel 群的满同态

$$\det=\tau\pi:\ \mathrm{K}_0(R)\twoheadrightarrow\mathrm{Pic}(R)$$

$$[M]\mapsto\langle\wedge^n N\rangle$$

其中 π,n,N 如命题 20.5 所示。当 R 为连通环时，$N=M$。

这个满同态 det 称为**行列式映射**(determinant map)。这个命名的含义可由下例看出。

例 1　设 $R\in\mathcal{C}\mathrm{Ring}$，$M=R^m$. 则 $f_M\in \mathrm{H}_0(R)$ 为常值函数：$f_M(P)=m$，$\forall P\in\mathrm{Spec}R$。此时 $\det([M])=\langle\wedge^m M\rangle=\langle\wedge^m R^m\rangle=\langle R\rangle$。

设 $A_1,A_2,\cdots,A_m$ 为 $M=R^m$ 之基，$A_j\in R^{m\times 1}$，则 $A_1\wedge\cdots\wedge A_m$ 为 $\wedge^m M\simeq R$ 之基。记 $A_M=(A_1\cdots A_m)\in R^{m\times m}$，则 A_M 为此基与标准基 $e_1,\cdots,e_m$ 间的演化矩阵。令 $e_1\wedge\cdots\wedge e_m=1=\mathrm{Det}(e_1\cdots e_m)$，则 $A_1\wedge\cdots\wedge A_m=\mathrm{Det}A_M\in R^{\cdot}$ 即通常的行列式。它给出了 R 的基，事实上完全确定了 $\det([M])=\langle R\rangle$。当 R 为域时，可令 $e_1\wedge\cdots\wedge e_m=a\neq 0$，此时 $A_1\wedge\cdots\wedge A_m$ 为通常行列式的 a 倍，即广义行列式。

从另一个角度看，由于这里的 $\wedge^m M\simeq R$，$\forall f\in\mathrm{End}_R M$，$\wedge^m(f)\in\mathrm{End}_R\wedge^m M\simeq R$，可视为 $\wedge^m(f)\in R$。这正是 Bourbaki 意义下的行列式定义。

注①　虽然可看出 $\forall F\in$ f. g. $\mathrm{Free}_R\mathfrak{M}$，$[F]\in\mathrm{Ker}\det$，因而 $\mathbb{Z}<\mathrm{Ker}\det$，求 $\mathrm{Ker}\det$ 仍是一件困难的事。即使在 R 是连通环时，上述的 $N=M$，问题转化为由 $\wedge^n N\simeq R$，$N\in$ f. g. $\mathrm{P}_R\mathfrak{M}$，如何确定 N 的结构，这也是困难的。

容易看出当 R 为连通环时，定理 19.2 中的 Abel 群单同态 $i:\mathrm{Pic}(R)\to$

$(K_0(R))^{\cdot}$ 与命题 21.1 中的 det 满足 $\det\cdot i = I_{\mathrm{Pic}(R)}$。但不能够由此断言：$\mathrm{Pic}(R)$ 同构于 $K_0(R)$ 的一个直和项，因为 $(K_0(R))^{\cdot}$（简记为 $K_0(R)^{\cdot}$）并非 $K_0(R)$（加法群）的子群。我们将在下节对 Dedekind 环给出圆满的答案。

思考题：什么时候 $\det[M_1 \bigotimes_R M_2] = \langle \wedge^{m_1} M_1 \rangle \langle \wedge^{m_2} M_2 \rangle$，$\forall M_j \in$ f. g. $P_R\mathfrak{M}$，$\mathrm{rank} M_j = m_j$？此时能否推出 $K_0(R)^{\cdot} \simeq \mathrm{Ker}\det \oplus \mathrm{Pic}(R)$？

关于 Pic 的函子性，我们有

命题 21.2 $\mathrm{Pic}: \mathcal{C}\mathrm{Ring} \to \mathcal{A}G$ 为共变函子。

证 在 $\mathcal{C}\mathrm{Ring}$ 中任取环同态 $g: R \to S$，定义

$$\mathrm{Pic}(g): \mathrm{Pic}(R) \to \mathrm{Pic}(S)$$
$$\langle M \rangle \mapsto \langle S \bigotimes_R M \rangle (= \langle S \bigotimes_R M \rangle)$$

由 $\mathrm{Pic}(R) < (K_0(R))^{\cdot}$，$K_0(g)$ 为环同态，再注意到对可逆 R-模 M，$\langle M \rangle = [M]$，即知

$$\mathrm{Pic}(g) = K_0(g) \mid_{\mathrm{Pic}(R)}$$

因此 $\mathrm{Pic}(g)$ 为完全确定的映射。容易看出 $\mathrm{Pic}(g)$ 又是群同态。

再直接验证函子的其他条件（保态射的合成，保恒等态射），即知本命题成立。 □

命题 21.3 $\det: K_0 \to \mathrm{Pic}$ 为函子 K_0 与 Pic 间的自然变换。

证 在 $\mathcal{C}\mathrm{Ring}$ 中任取环同态 $g: R \to S$，只需证明

$$\begin{array}{ccc} K_0(R) & \xrightarrow{K_0 g} & K_0(S) \\ \det \downarrow & & \downarrow \det \\ \mathrm{Pic}(R) & \xrightarrow[\mathrm{Pic}\, g]{} & \mathrm{Pic}(S) \end{array}$$

为交换图。事实上 $\forall [M] \in K_0(R)$，用命题 20.5 中的 N（由 M 确定）与命题 21.1 直接验证即可。 □

注② 可以证明（比如见[Bass，1968]）：设 $R \in \mathcal{C}\mathrm{Ring}$，则

（1）当 $\mathrm{Max}R$ 为维数 $\leqslant 1$ 的 Noether 空间（比如 R 为 Noether 环且 K. $\dim R \leqslant 1$，特别地，R 为 Dedekind 环）时，$\det: rK_0(R) \to \mathrm{Pic}(R)$ 为群同构；

（2）下述三点等价：

（a）$\det: rK_0(R) \to \mathrm{Pic}(R)$ 为群同构；（b）若 $P \in$ f. g. $P_R\mathfrak{M}$ 且 $\mathrm{rank}P = r$，则 $P \lesssim \wedge^r P \oplus R^{r-1}$（稳定同构）；（c）有常数秩的有限生成投射 R-模必为可逆 R-模的（有限）直和，且对任意的可逆 R-模 M, N，$M \oplus N \lesssim (M \bigotimes_R N) \oplus R$。由此结果可知：对 Dedekind 环 R，$\forall I, J \lhd R$，$I \oplus J \simeq (I \bigotimes_R J) \oplus R \simeq IJ \oplus R$（在 §22 将给出直接证明）。

下面我们讨论整环的 Picard 群。

设 R 为整环，$F=Q(R)$ 为 R 的分式域，则 $F\in {}_R\mathfrak{M}$，且 $\forall I\lhd R$，I 都是 F 的 R-子模，记为 $I<F$。先来证明

命题 21.4　设 R 为整环，则

$$\begin{aligned}\mathrm{Pic}(R)&\equiv\{\langle M\rangle\mid M\text{ 为可逆 }R\text{-模}\}\\&=\{\langle M\rangle\mid 0\neq M\in \mathrm{f.g.\,P}_R\mathfrak{M}\text{ 且 }M\underset{R}{<}F\}\end{aligned}$$

证　(1) 设 $\langle M\rangle\in\mathrm{Pic}(R)$，即 M 为可逆 R-模，由定义 19.1 与定理 19.1 知 $0\neq M\in\mathrm{f.g.\,P}_R\mathfrak{M}$，又由 R 为整环知 $0\in\mathrm{Spec}R$ 且 $M_0\simeq R_0=F$，下证标准同态

$$f:M\to M_0$$
$$m\mapsto\frac{m}{1}$$

为单射，即知 $\mathrm{Pic}(R)\subseteq\{\langle M\rangle\mid 0\neq M\in\mathrm{f.g.\,P}_R\mathfrak{M}\text{ 且 }M\underset{R}{<}F\}$。

事实上，$\frac{m}{1}=0\Leftrightarrow$ 有 $0\neq t\in R$ 使 $tm=0$。但 $M\in\mathrm{P}_R\mathfrak{M}\subset$ $\mathrm{Flat}_R\mathfrak{M}$ 而整环上的平坦模都是无挠的。因此 $m=0$，即 f 为单射。

(2) 再证反向包含关系。设 $M\underset{R}{<}F$ 且 $0\neq M\in\mathrm{f.g.\,P}_R\mathfrak{M}$。任取 $\frac{r}{s}\in M\backslash\{0\}$，定义

$$g:F\to M_0$$
$$\frac{t}{u}\mapsto\left(\frac{tr}{s}\right)/u\ \left(=\frac{t}{u}\cdot\frac{r}{s}\right)$$

若 $\frac{t}{u}=\frac{t_1}{u_1}$，则

$$g\left(\frac{t_1}{u_1}\right)=\left(\frac{t_1r}{s}\right)/u_1=\left(\frac{tr}{s}\right)/u=\frac{t}{u}\cdot\frac{r}{s}=g\left(\frac{t}{u}\right)$$

这说明 g 为完全确定的映射。又可直接验证 g 为 R-模同构。于是 $F\underset{R}{\simeq}M_0$，即 $\mathrm{rank}_0M=1$。但 R 为连通环，因此 $\mathrm{rank}M=1$。于是 M 为可逆 R-模。由此即知 $\{\langle M\rangle\mid 0\neq M\in\mathrm{f.g.\,P}_R\mathfrak{M}\text{ 且 }M\underset{R}{<}F\}\subseteq\mathrm{Pic}(R)$，从而命题证毕。　□

由于 $\forall I\lhd R$，$I\underset{R}{<}F$，可将理想的概念推广如下。

定义 21.1　设 R 为整环，$F=Q(R)$ 为 R 的分式域。若 $0\neq M\underset{R}{<}F$ 且有 $0\neq J\lhd R$ 与 $c\in F^{\cdot}$ 使 $M=cJ$，则称 M 为 R 的**分式理想**(fractional ideal)，记为 $M\in\mathrm{FI}(R)$ 或简记为 $M\in\mathrm{FI}$。$J=R$ 时，即 $M\doteq cR$ 形的分式理想又称为**主分式理想**，记为 $M\in\mathrm{PFI}(R)$ 或 $M\in\mathrm{PFI}$。$c=1$ 时，即 R 的理想又称为**整**

分式理想。

由定义知，$\mathrm{FI}(\mathbb{Z})=Q^{\cdot}(n)$，$\forall 0\neq n\in\mathbb{Z}$($\mathbb{Z}$ 中的理想都是主理想，可表如(n))。因此$\mathbb{Z}$ 的分式理想都可表为$(\frac{r}{s})=\frac{r}{s}\mathbb{Z}=\{\frac{mr}{s}\mid 0\neq r,s\in\mathbb{Z},m\in\mathbb{Z}\}$之形，此时 $\mathrm{FI}(\mathbb{Z})=\mathrm{PFI}(\mathbb{Z})$，但一般地，$\mathrm{FI}(R)=\{cJ\mid\forall 0\neq J\lhd R,c\in F^{\cdot}\}\supset\mathrm{PFI}(R)=\{cR\mid c\in F^{\cdot}\}$。

对分式理想可作如下刻画。

命题 21.5 设 R 为整环，$F=Q(R)$为 R 的分式域，$0\neq M\underset{R}{<}F$，则下述各点等价：

$(1)_1$ $M\in\mathrm{FI}$；

$(1)_2$有 $c_1\in F^{\cdot}$ 使 $c_1M\lhd R$ $(c_1M\subseteq R)$；

$(2)_1$有 $0\neq d\in R$ 使 $dM\subseteq R$；

$(2)_2$有 $0\neq d\in R$ 使 $dM\lhd R$；

(3) 有 $a,b\in F^{\cdot}$ 使 $aR\subseteq M\subseteq bR$。

证 $(1)_1\Leftrightarrow(1)_2$，$(2)_1\Leftrightarrow(2)_2$ 是显见的。

$(1)_2\Rightarrow(2)_2$：令 $c_1=\frac{r}{s}$，取 $d=sc_1=r$ 即可。

$(2)_1\Rightarrow(3)$：$dM\subseteq R\Rightarrow M\subseteq d^{-1}R$。

取 $0\neq m\in M\underset{R}{<}F$，由 $M\in{}_R\mathfrak{M}_R$ 知 $mR\subseteq M$。

于是令 $b=d^{-1}$，$a=m$，即得(3)。

$(3)\Rightarrow(1)_1$：令 $J=b^{-1}M$，则 $0\neq J\lhd R$，且 $M=bJ$。因此 $M\in\mathrm{FI}$。 □

由此命题容易得出如下推论。

推论 21.1 设 R 为整环，$R=Q(R)$为 R 的分式域，则

(1) F 的非零有限生成子 R-模都是 R 的分式理想；

(2) 当 R 又为 Noether 环时，$\mathrm{FI}=\{M\mid 0\neq M\underset{\text{f.g.}}{<}F\}$；

(3) 任一分式理想，作为 R-模都同构于 R 的一个非零理想；

(4) $\mathrm{FI}(R)$按乘法 $MN=\{\sum_{<\infty}m_jn_j\mid m_j\in M,n_j\in N\}$ 为交换幺半群，单位元为 R 。

建议读者考虑：幺半群 $\mathrm{FI}(R)$的群完备化是什么？

在下节我们将证明：$\mathrm{FI}(R)$为群$\Leftrightarrow R$ 为 Dedekind 环。由下一推论可看出，一般地，每一个分式理想都是“半可逆”的。

推论 21.2 设 R 为整环，F 为 R 的分式域，$M\in\mathrm{FI}(R)$，记

$$\overline{M}=\{x\in F\mid xM\subseteq R\}\equiv(R:M)$$

则 $\overline{M}\in FI(R)$ 且 $M\overline{M}=\overline{M}M\subseteq R$。

证　$\overline{M}\underset{R}{<}F$ 是显见的. 又由 $M\in \mathrm{FI}(R)$ 知,$0\neq M=cJ$,其中 $c\in F^{\cdot}$,$J\lhd R$。因此,$c^{-1}\in\overline{M}$,由此知 $0\neq\overline{M}$,于是 $0\neq\overline{M}\underset{R}{<}F$。

又由 $M\neq 0$ 知可取 $0\neq m\in M$,于是 $m\in F^{\cdot}$ 且 $m\overline{M}\subseteq R$,由命题 21.5 知,$\overline{M}\in \mathrm{FI}(R)$。

再由 $\overline{M}$ 的定义与 $R\in \mathcal{C}\mathrm{Ring}$ 又可知 $M\overline{M}=\overline{M}M\subseteq R$。　□

定义 21.2　设 R 为整环,若 $M\in \mathrm{FI}(R)$ 使 $M\overline{M}=R$(此时必有 $\overline{M}M=R$),则称 M 为 R 的**可逆分式理想**(invertible fractional ideal),记为 $M\in \mathrm{FI}^{\cdot}$,同时记 $M^{-1}=\overline{M}$。

显然 $\mathrm{FI}^{\cdot}\in \mathcal{A}G$ 且单位元为 R,同时 $\mathrm{PFI}\lhd \mathrm{FI}^{\cdot}$。

对可逆分式理想,有如下的特征刻画。

命题 21.6　设 R 为整环,F 为 R 的分式域,则 $M\in \mathrm{FI}^{\cdot}\Leftrightarrow M\in \mathrm{f.g.}\,\mathrm{P}_R\mathfrak{M}$ 且 $0\neq M\underset{R}{<}F$。因此

$$\mathrm{FI}^{\cdot}=\{F\text{ 的非零有限生成的投射子 }R\text{- 模}\}$$

证　$\Rightarrow$:由 $M\in FI^{\cdot}$ 即 $M\overline{M}=R$ 知,必有 $m_j\in M,\overline{m}_j\in\overline{M}$ 使

$$1=m_1\overline{m}_1+m_2\overline{m}_2+\cdots+m_r\overline{m}_r$$

由此可定义两个 R-模同态

$$i:M\to R^r$$
$$m\mapsto(m\overline{m}_1,\cdots,m\overline{m}_r),$$
$$\pi:R^r\to M$$
$$(x_1,\cdots,x_r)\mapsto x_1m_1+\cdots+x_rm_r。$$

容易看出 $\pi i=\mathrm{I}_M$. 因此

$$R^r=\mathrm{Im}i\oplus\mathrm{Ker}\pi\simeq M\oplus\mathrm{Ker}\pi$$

于是 $M\in \mathrm{f.g.}\,\mathrm{P}_R\mathfrak{M}$。而由 $M\in FI$ 又知 $0\neq M\underset{R}{<}F$。

$\Leftarrow$:设 $M\in \mathrm{f.g.}\,\mathrm{P}_R\mathfrak{M}$ 且 $0\neq M\underset{R}{<}F$,则由推论 21.1(1)知 $M\in \mathrm{FI}$,只需再证 $M\overline{M}=R$。但由推论 21.2 已知 $M\overline{M}\subseteq R$,故只需再证 $R\subseteq M\overline{M}$,即证 $1\in M\overline{M}$。

事实上,由 $M\in \mathrm{f.g.}\,\mathrm{P}_R\mathfrak{M}$,可令 $R^r\simeq M\oplus N$。于是有单同态

$$i:M\to R^r$$
$$m\mapsto(x_1,\cdots,x_r)$$

与满同态

$$\pi:R^r\twoheadrightarrow M$$

使 $\pi i=I_M$.

取 R-模同态

$$f_j: M \to R$$
$$m \mapsto x_j$$

且记 $m_1=\pi(1,0,\cdots,0),\cdots,m_r=\pi(0,\cdots,0,1)$，于是

$$m = \pi i(m) = \sum_{j=1}^{r} f_j(m) m_j, \qquad \forall m \in M$$

但 $M \underset{R}{<} F$。于是对任意的 $m, m' \in M$（通分后）必有 $a, a', s \in R$ 使 $m=\frac{a}{s}$，$m'=\frac{a'}{s}$。从而有

$$m f_j(m') = \frac{a}{s} f_j\left(\frac{a'}{s}\right) = \frac{1}{s} f_j\left(\frac{aa'}{s}\right) = \frac{a'}{s} f_j\left(\frac{a}{s}\right) = m' f_j(m)$$

令 $m \neq 0$，$n_j = m^{-1} f_j(m) \in F$，则 $f_j(m) = mn_j \in R$，$\forall 0 \neq m \in M$。因此 $Mn_j \subseteq R$，即 $n_j \in \overline{M}$，$j=1,2,\cdots,r$。但由上

$$m = \sum_{j=1}^{r} f_j(m) m_j = \sum_{j=1}^{r} m n_j m_j$$
$$= m \sum_{j=1}^{r} n_j m_j, \qquad \forall 0 \neq m \in M \underset{R}{<} F$$

两边以 m^{-1} 乘之，即得

$$1 = \sum_{j=1}^{r} n_j m_j = \sum_{j=1}^{r} m_j n_j \in M\overline{M}$$ □

命题 21.7 设 R 为整环，F 为 R 的分式域，$M \in \mathrm{FI}^{\cdot}$，则

(1) $\overline{\overline{M}} = M$，即 ${M^{-1}}^{-1} = M$；

(2) $N \underset{R}{<} F$ 使 $MN = R$ 时，$N = \overline{M}$（即 M^{-1} 惟一）；

(3) $N \in \mathrm{FI}^{\cdot}$ 时，$\overline{MN} = \overline{M}\,\overline{N}$，即 $(MN)^{-1} = M^{-1}N^{-1}$；

(4) $N \in \mathrm{FI}^{\cdot}$ 时，必有 R-模同构 $g: M \underset{R}{\otimes} N \to MN$ 使

$$g\left(\sum_{<\infty}(m_j \otimes n_j)\right) = \sum_{<\infty} m_j n_j, \qquad \forall m_j \in M,\ n_j \in N;$$

(5) $\overline{M} \simeq M^* = \mathrm{Hom}_R(M, R)$。因此，当 $0 \neq N \underset{R}{<} F$ 时，N 为 R 的可逆分式理想（$N \in \mathrm{FI}^{\cdot}$）$\Leftrightarrow N$ 为可逆 R-模 $\Leftrightarrow N \in \mathrm{f.g.}\,\mathrm{P}_R\mathfrak{M}$；

(6) $\mathrm{Pic}(R) = \{\langle M \rangle \mid M \in \mathrm{FI}^{\cdot}\}$。

证 (1)、(2)、(3)是逆元素的性质（注意 $\mathrm{FI}^{\cdot} \in \mathcal{AG}$），不必再证。

(4) 由 $M, N \in \mathrm{FI}^{\cdot}$ 知，$MN \in \mathrm{FI}^{\cdot}$。

对任意的 $X \in \mathrm{FI}^{\cdot}$，则由命题 21.6 知 $0 \neq X \underset{R}{<} F$ 且 $X \in \mathrm{f.g.}\,\mathrm{P}_R\mathfrak{M}$，再由

命题 21.4 之证的(2)可知,有 R-模同构 $X_0 \simeq F$,于是 $\mathrm{rank}_0 X=1$。但 R 为连通环,因此 $\mathrm{rank}X=1$。由此即知 $M,N,MN,M\bigotimes_R N$ 都有常数秩 1。再注意 g 显然为满同态,于是由推论 19.2 即知 g 为 R-模同构。

(5) 由(4)知(取 $N=\overline{M}$),

$$M\bigotimes_R \overline{M} \simeq M\overline{M} = R$$

于是由定理 19.1 即知 $\overline{M}\simeq M^*$。

(6) 由命题 21.4 与命题 21.6 即得。 □

与 Picard 群有紧密联系的是理想类群。

设 R 为整环,记

$$\mathrm{Cl}(R) = \{\langle I\rangle \mid 0 \neq I \lhd R, I \in \mathrm{f.g.}\ \mathrm{P}_R\mathfrak{M}\}$$

规定其运算为

$$\langle I\rangle\langle J\rangle = \langle IJ\rangle, \qquad \forall \langle I\rangle,\langle J\rangle \in \mathrm{Cl}(R)$$

则 Cl(R)为 Abel 幺半群。显然 $\mathrm{Cl}(R)\subseteq\mathrm{Pic}(R)$。下面来证明更进一步的结果。

推论 21.3　设 R 为整环,则

$$\mathrm{Cl}(R) = \{\langle I\rangle \mid 0 \neq I \lhd R, I \in \mathrm{FI}^{\cdot}\}$$

为(乘法)Abel 群,同时 $\mathrm{Cl}(R)\simeq\mathrm{Pic}(R)$。

证　$\forall\, 0\neq I\lhd R, I\underset{R}{<}F$($R$ 的分式域)。于是由命题 21.6 知,$I\in \mathrm{FI}^{\cdot}$ 当且仅当 $I\in \mathrm{f.g.}\ \mathrm{P}_R\mathfrak{M}$。因此

$$\mathrm{Cl}(R) = \{\langle I\rangle \mid 0 \neq I \lhd R,\ I \in \mathrm{FI}^{\cdot}\}$$

从定义 21.1 又知,$\forall M\in \mathrm{FI}$ 都有 $c\in F^{\cdot}$,$I\lhd R$ 使 $M=cI$。因此,作为 R-模 $M\simeq I$。于是从命题 21.7(6)即知 $\mathrm{Cl}(R)\simeq\mathrm{Pic}(R)$。 □

由此推论可给出如下定义。

定义 21.3　设 R 为整环,则称 Cl(R)为 R 的**理想类群**(ideal class group),或简称为 R 的**类群**(class group),其阶数(元素个数)称为 R 的**类数**(class number),记为 h_R 或 h。

容易看出,当 R 为 PID, UFD 或交换整半局部环时,$\mathrm{Cl}(R)\simeq\mathrm{Pic}(R)$ $(=1)$都是平凡的。

注③　整环上的 Picard 群的研究起源于代数几何。一个仿射代数簇(指一个多元多项式方程组的解集是既约的,比如既约代数曲线,既约代数曲面)的坐标环 $A[V]$都是整环,对既约无奇点的代数曲线、或既约无奇点的代数曲面 V(或更一般地,对正规的仿射代数簇,即坐标环在每一极大理想的局部化都是关于其商域整闭的仿射的代数簇 V),记 V 的上维数(codi-

mension)为 1 的子簇的集合为 $\mathscr{P}$,以 $\mathscr{P}$ 作基的自由 Abel 群记为 $D(V)$(其元素称为(Weil)**除子**(divisor)),对 V 上的任意非 0 有理函数 f(模去 V 的定义方程组中的多元多项式之余),即 f 为 $A[V]$之商域(分式域)$A(V)$的元素,与任一个 $w\in\mathscr{P}$,记 $v_w(f)\in\mathbb{Z}$ 为 f 沿着(关于)w 的零点阶数减去 f 沿着 w 的极点阶数,并记

$$\mathrm{div}(f)=\sum_{w\in\mathscr{P}}v_w(f)\cdot w$$

称为 f 对应的**主除子**(principal divisor),也记为(f)。按$(fg)=(f)+(g)$,$(f/g)=(f)-(g)$,得到一个主除子群 $P(V)$,它是 $D(V)$的子群(正规子群)。

$$C(V)\equiv D(V)/P(V)$$

称为 V 的**除子类群**(divisor class group)(属同一个陪集的除子称为是线性等价的)。如果 $M\in D(V)$对 V 的每点的一个邻域,都是对应一个有理函数 f 的除子,则称 M 为 **Cartier 除子**。Cartier 除子生成 $D(V)$的一个子群,这个子群关于线性等价所成的商群称为 V 的 Picard 群,记为 $\mathrm{Pic}(V)$。可证明 $\mathrm{Pic}(V)\simeq\mathrm{Pic}A[V]$。$V$ 是光滑的(smooth)(即无奇点)时候,$C(V)=\mathrm{Pic}(V)$,当 $A[V]$为 Dedekind 环(如光滑的平面代数曲线 V 的坐标环 $A[V]$)时

$$\mathrm{Cl}(A[V])\simeq C(V)=\mathrm{Pic}(V)\simeq\mathrm{Pic}(A[V])$$

由上我们已看出:设 R 为整环,则

$$\begin{aligned}\mathrm{Cl}(R)&=\{\langle I\rangle\mid 0\neq I\lhd R,I\in\mathrm{FI}^{\cdot}\}\\&\simeq\mathrm{Pic}(R)=\{\langle M\rangle\mid M\in\mathrm{FI}^{\cdot}\}\end{aligned}$$

下一结果说明对 $\mathrm{FI}^{\cdot}$ 取同构类相当于 $\mathrm{FI}^{\cdot}$ 模去 PFI。

定理 21.1 设 R 为整环,则

$$\mathrm{Pic}(R)\simeq\mathrm{Cl}(R)\simeq\mathrm{FI}^{\cdot}/\mathrm{PFI}$$

证 $\forall M\in\mathrm{FI}^{\cdot}$,必有 $c\in F^{\cdot}$ 使 $M=cI,0\neq I\lhd R$。即,作为 R-模,$M\simeq I\lhd R,I\in\mathrm{FI}^{\cdot}$。反过来,$\forall\langle I\rangle\in\mathrm{Cl}(R)$,可令 $0\neq I\lhd R,I\in\mathrm{FI}^{\cdot}$。因此有 Abel 群的满同态

$$\begin{aligned}\pi:\mathrm{FI}^{\cdot}&\twoheadrightarrow\mathrm{Cl}(R)\\M&\mapsto\langle I\rangle,M=cI,c\in F^{\cdot}\end{aligned}$$

注意 $\mathrm{Cl}(R)$的单位元为$\langle R\rangle$,可知

$$\mathrm{Ker}\pi=\{cR\mid c\in F^{\cdot}\}=\mathrm{PFI}$$

于是

$$\mathrm{Pic}(R)\overset{\text{推论21.3}}{\simeq}\mathrm{Cl}(R)\simeq\mathrm{FI}^{\cdot}/\mathrm{PFI}$$ □

由此定理及其上述证明立得

推论 21.4　设 R 为整环，则

$$\mathrm{Pic}(R) \simeq \mathrm{Cl}(R) = \{\langle R\rangle, \langle I\rangle \mid 0 \neq I \subsetneqq R \text{ 非主理想}, I \in \mathrm{FI}^{\cdot}\}$$

这个结果在形式上给出了 Picard 群与理想类群最"经济"的算法。

推论 21.5　设 R 为整环，则有 Abel 群($\mathbb{Z}$-模)的两个正合列

$$1 \to R^{\cdot} \to F^{\cdot} \longrightarrow \mathrm{FI}^{\cdot} \to \mathrm{Cl}(R) \to 1$$

$$u \longmapsto uR$$

$$1 \to R^{\cdot} \to F^{\cdot} \longrightarrow FI^{\cdot} \to \mathrm{Pic}(R) \to 1$$

$$u \longmapsto uR$$

为使读者更清楚地认识需弄清的一些概念，我们列出下述的蕴含关系图(设 R 为整环，F 为 R 的分式域)：

$$\mathrm{PFI} \subset \mathrm{FI}^{\cdot} = \{M \mid 0 \neq M \underset{\mathrm{f.g.P}}{<} F\} \subset \{M \mid 0 \neq M \underset{\mathrm{f.g.}}{<} F\} \subset \mathrm{FI} = \{M \mid 0 \neq M = cJ,\ J \lhd R,\ c \in F^{\cdot}\}$$

$\cap$　　　　　　　　　　　　　　　　　　$\cup$

{可逆 R-模}　　　　　　　　　　　　{整分式理想} $= \{J \mid 0 \neq J \lhd R\}$

由过去对 $\mathcal{C}$Ring 关于 K_0 环的结果，很容易得出关于 Picard 群的相应结果。比如，我们有

命题 21.8　设在 $\mathcal{C}$Ring 中，$\pi: R \to S$ 为环的满同态，而且 $\mathrm{Ker}\pi = I \subseteq J(R)$。则有群的单同态 $\mathrm{Pic}(\pi): \mathrm{Pic}(R) \to \mathrm{Pic}(S)$。因此当 $\mathrm{Pic}(S) = 1$ 时，必有 $\mathrm{Pic}(R) = 1$。

证　由定理 3.1 知 $K_0(\pi)$ 为单同态，而 $\mathrm{Pic}(R) < K_0(R)^{\cdot}$，于是 $\mathrm{Pic}(\pi) = K_0(\pi)|_{\mathrm{Pic}(R)}: \mathrm{Pic}(R) \to \mathrm{Pic}(S)$。由此即得欲证。　□

命题 21.9　设在 $\mathcal{C}$Ring 中，环同态 $f: R \to S$ 与 $g: S \to R$ 使 $gf = I_R$，则在同构意义下，$\mathrm{Pic}(R)$ 为 $\mathrm{Pic}(S)$ 的直和项。

证　用 Pic 的函子性仿命题 2.5 之证。

命题 21.10　设 $R, R_j \in \mathcal{C}\mathrm{Ring}$，$R \simeq R_1 \oplus \cdots \oplus R_n$，则有群同构 $\mathrm{Pic}(R) \simeq \mathrm{Pic}(R_1) \oplus \cdots \oplus \mathrm{Pic}(R_n)$，因此 $\mathrm{Pic}(R) = 1 \Leftrightarrow \mathrm{Pic}(R_j) = 1, j = 1, 2, \cdots, n$。

证　仿上用命题 2.6。

命题 21.11　设 $\{R_\alpha, f_{\beta\alpha}: R_\alpha \to R_\beta, \alpha \leqslant \beta, \alpha, \beta \in \Lambda\}$ 为 $\mathcal{C}$Ring 中的正向系，Λ 为正向集，则

$$\mathrm{Pic}(\varinjlim R_\alpha) \simeq \varinjlim \mathrm{Pic}(R_\alpha)$$

证　仿上用定理 13.1。

§ 22　Dedekind 环上 K_0 群的四种分解

在代数几何中，平面代数曲线 V 无奇点（光滑）的充要条件是其坐标环 $A[V]$ 为 Dedekind 环。在代数数论中，代数数域 F（$\mathbb{Q}$ 的有限次扩张）的代数整元环 O_F 也是 Dedekind 环，比如分圆域 $Q(\xi_n)$（ξ_n 为 n 次本原单位根）的代数整元环 $\mathbb{Z}[\xi_n]$ 以及（实、虚）二次域的代数整元环，都是 Dedekind 环。因此 Dedekind 环在代数几何与代数数论中有重要应用。由于 Dedekind 环的重要性，虽然过去我们已几次用到或提到 Dedekind 环。这里我们仍将 Dedekind 环丰富的特征刻画给出，以便于应用与掌握。熟悉 Dedekind 环的读者可跳过下面的证明，不必再读。

定义 22.1　设 R 为整环，且 $\forall I \underset{\neq}{\lhd} R$，$I$ 都为有限个素理想之积，则称 R 为 Dedekind（整）环（Dedekind domain）。

定理 22.1　设 R 为整环，则下述各点是等价的：

(1) R 为 Dedekind 环；

$(2)_1$ $\forall 0 \neq P \in \mathrm{Spec}R$，$P \in \mathrm{Max}R$ 且 $P \in \mathrm{FI}^{\cdot}$；

$(2)_2$ $\forall 0 \neq P \in \mathrm{Spec}R$，$P \in \mathrm{FI}^{\cdot}$；

(3) $\forall 0 \neq I \underset{\neq}{\lhd} R$，有惟一的 $P_1, P_2, \cdots, P_n \in \mathrm{Spec}R$ 使 $I = P_1 P_2 \cdots P_n$；

(4) $\forall I, J \lhd R$，若 $I \subseteq J$，则必有 $I_1 \lhd R$ 使 $I = I_1 J$；

(5) $\forall 0 \neq I \lhd R$，$I \in \mathrm{FI}^{\cdot}$；

(6) FI 为乘法群；

(7) $\mathrm{FI} = \mathrm{FI}^{\cdot}$；

(8) $\forall I \lhd R$，$I \in \mathrm{f.g.}\, \mathrm{P}_R\mathfrak{M}$；

(9) R 为遗传环（即 $\forall I \lhd R$，$I \in \mathrm{P}_R\mathfrak{M}$），即 $gD(R) \leqslant 1$；

(10) $\mathrm{FI} \subseteq \mathrm{P}_R\mathfrak{M}$；

(11) R 为 Noether 环，$\{0\} \cup \mathrm{Max}R = \mathrm{Spec}R$（即 $\mathrm{Kdim}R \leqslant 1$）且 R 为整闭的（即 $R = \{r \in F = Q(R) \mid$ 有首一的 $f(x) \in R[x]$ 使 $f(r) = 0\} \equiv \bar{R}$（$R$ 的代数整闭包））；

(12) R 为 Noether 环，且 $\forall 0 \neq P \in \mathrm{Spec}R$，$R_P \in \mathrm{DVR}$（离散赋值环，即恰有一个非零素理想的 PID）。

证　$(1) \Rightarrow (2)_1$：先证①：R 中可逆素理想 P 必是极大理想。

任取 $a \in R \backslash P$ 来证 $P + Ra = R$ 即可。反设 $P + Ra \neq R$，则 $P + Ra^2 \neq R$，

于是由(1)有素理想分解

$$P + Ra = P_1 P_2 \cdots P_m,$$

$$P + Ra^2 = Q_1, Q_2, \cdots, Q_n$$

在标准环同态 $\pi: R \to R/P$ 之下，记 $\bar{a} = \pi(a)$，$\bar{J} = \pi(J)$，$\forall J \lhd R$，则在 R/P 中有素理想分解

$$(\bar{a}) = \bar{P}_1 \cdots \bar{P}_m,$$

$$(\bar{a}^2) = \bar{Q}_1 \cdots \bar{Q}_n$$

由 R/P 为整环知$(\bar{a})$，$(\bar{a}^2)$都可逆，因此 $\bar{P}_i$，$\bar{Q}_j$ 都可逆。由此经排序后可得 $n = 2m$ 且

$$\bar{P}_i = \bar{Q}_{2i} = \bar{Q}_{2i-1}, \qquad i = 1, 2, \cdots, m$$

因此 $P + Ra^2 = (P + Ra)^2$。由此知

$$P \subseteq P + Ra^2 = (P + Ra)^2 \subseteq P^2 + Ra$$

即 $\forall b \in P$ 都可表为 $b = c + ra$，$c \in P^2 \subseteq P$，于是 $ra \in P$。但 $a \notin P$，故 $r \in P$，即

$$P \subseteq P^2 + Pa \subseteq P$$

由此知 $P = P^2 + Pa$。再由 P 可逆则又得 $P + Ra = R$，矛盾。

② 任取 $0 \neq c \in P \in \mathrm{Spec}R$. 由(1)知$(c)$有素理想分解

$$(c) = P_1' \cdots P_k' \subseteq P$$

因此必有 $P_j' \subseteq P$。又由(c)可逆知 P_j' 可逆。于是由①知 $P_j' \in \mathrm{Max}R$，故 $P_j' = P$，于是 P 可逆。

$(2)_1 \Rightarrow (2)_2$ 是当然的。

$(2)_2 \Rightarrow (3)$：由$(2)_2$ 知 R 为 Noether 环(因为一切素理想都是有限生成的)。反设(3)不成立，则 R 中不能惟一分解(为素理想之积)的理想集必有极大元 $J \neq R$。因此必有 $P \in \mathrm{Max}R$ 使 $J \subsetneq P$。由 $JP \subseteq J$，P^{-1} 存在知 $J \subseteq JP^{-1} \subseteq R$，注意 $JP^{-1} \neq R$(否则 $J = P$，与 J 的选取矛盾)。若 $J \subsetneq JP^{-1}$，则 $JP^{-1} \lhd R$ 可惟一分解，于是以 P 乘分解式得 J 的惟一分解，此与 J 的选取矛盾。于是 $J = JP^{-1}$，即 $JP = J$。只需由此引出矛盾即可。事实上，可令 $J = \langle x_1, x_2, \cdots, x_m \rangle \underset{\text{f.g.}}{\lhd} R$. 于是有

$$x_j = p_{j1} x_1 + \cdots + p_{jn} x_n, \qquad j = 1, \cdots, n,\ p_{ij} \in p$$

即

$$\begin{pmatrix} p_{11} - 1 & p_{12} & \cdots & p_{1n} \\ \cdots & \cdots & \cdots & \cdots \\ p_{n1} & p_{n2} & \cdots & p_{nn} - 1 \end{pmatrix} \begin{pmatrix} x_2 \\ \cdots \\ x_n \end{pmatrix} = 0$$

由 R 为整环与 $x_1,\cdots,x_n$ 不全为 0 知 $\det(p_{ij})=0$，于是 $1\in P$，矛盾。

(3)⇒(1)是当然的。于是(1)⇔$(2)_i$⇔(3)，$i=1,2$。

又有显见或由上节可看出的关系：

(5)⇔(6)⇔(7)⇔(8)⇒(9)⇔(10)。

(10)⇒(7)：$\forall M\in \mathrm{FI}$，由(10)可令 M 为 R^S（S 可为无穷集）的直和项。取 $0\neq m\in M$，仿命题 21.7 之证，注意 $i(m)\in R^S$ 只有有限个分量不为 0 即可。因此(10)⇒(7)。由此知(5)，…，(10)都是等价的。

(5)⇒(4)：取 $I_1=J^{-1}I$ 即可。

(4)⇒(5)：$\forall\, 0\neq I\lhd R$，由(4)，取 $0\neq a\in I$，则知有 $I_1\lhd R$ 使 $(a)=II_1$，但 $(a)\in \mathrm{FI}^*$（R 为整环）。于是 $R=I(I_1(a)^{-1})$ 即 $I\in\mathrm{FI}^*$。

由此知(4)，(5)，…，(10)都是等价的。

(5)⇒(1)：由(5)已知 R 为 Noether 环，用$(2)_2$⇒(3)之证法即可。

(2)，(3)⇒(4)是显见的。于是(1)，(2)，…，(10)都是等价的。

(1)—(10)⇒(11)：由(2)已得 $\mathrm{Spec}R=\{0\}\cup\mathrm{Max}R$，由(5)知 R 为 Noether 环。只需再证 R 为整闭的，即任取 $u\in F$（R 的分式域）为 R 上的代数整元。证 $u\in R$ 即可，为此只需证 $R[u]=R$。

注意 $R[u]\underset{\text{f. g.}}{<}F$（作为 R-模），于是 $R[u]\in\mathrm{FI}$。由(7)知 $R[u]\in\mathrm{FI}^*$。但 $R[u]R[u]=R[u]$。于是

$$R[u]=RR[u]=(R[u]^{-1}R[u])R[u]=R[u]^{-1}R[u]=R$$

(11)⇒(12)：由 R 为整闭的知 R_P 为整闭的。而 R_P 的理想都可表为

$$I_P=\{\frac{i}{s}\mid i\in I\lhd R,S\in R\backslash P\}$$

但 R 为 Noether 环，$I\underset{\text{f. g.}}{\lhd}R$，于是 R_P 为 Noether 环。又由

$$\mathrm{Spec}R_P=\{Q_P\mid P\supset Q\in\mathrm{Spec}R=\mathrm{Max}R\cup\{0\}\}$$

知，R_P 有惟一的非零素理想 P_P。容易验证 R_P 仍为 Dedekind 环。因此，$\forall\,0\neq I_P\lhd R_P$，有 n 使 $I_P=P_P^n$。因此只需证 R_P 为主理想即可。

事实上，由 P_P 可逆知 $P_P^2\subsetneq P_P$。于是有 $0\neq a\in R_P\backslash P_P^2$，$0\neq aP_P^{-1}\lhd R_P$，但 $aP_P^{-1}\not\subset P_P$（否则，有 $a\in P_P^2$ 矛盾），故 $aP_P^{-1}=R_P$，即 $P_P=aR_P$ 为主理想。

(12)⇒(5)：$\forall\,0\neq I\lhd R$，由推论 21.2 知 $0\neq I\bar{I}\lhd R$。若 $I\bar{I}\neq R$，则有 $Q\in\mathrm{Max}R$ 使 $I\bar{I}\subseteq Q$。由(12)知 I_Q 为 R_Q 中主理想，于是可令 $I_Q=(\frac{a}{s})$，$a\in I$，$s\in R\backslash Q$. 但 R 为 Noether 环，I 必为有限生成的，可令 $I=(b_1,\cdots,b_n)$. 于是 $\frac{b_j}{1}\in I_Q$ 可表为

$$\frac{b_j}{1} = \frac{r_j}{s_j} \cdot \frac{a}{s}, \qquad r_j \in R,\ s_j \in R\backslash Q$$

记 $t = s_1 s_2 \cdots s_n$，则 $t \in R\backslash Q$，且在 F(R 的分式域)中

$$\frac{t}{a} \cdot b_j = \frac{tb_j}{a} = s_1 \cdots s_{j-1} s_{j+1} \cdots s_n r_j a \in I \subseteq R, \quad \forall j = 1,2,\cdots,n$$

因此 $t/a \in \bar{I}$，$t = (t/a)a \in \bar{I}I = I\bar{I} \subseteq Q$，与 $t \notin Q$ 矛盾，故 $I\bar{I} = R$。即(5)成立，从而定理证毕。 □

由上面$(2)_2 \Rightarrow (3)$的证法可得一个有用的工具。

推论 22.1 (也称为 Nakayama 引理)。设 $R \in \mathcal{C}\mathrm{Ring}$，$M \in \mathrm{f.g.}\,{}_R\mathfrak{M}$，$I \lhd R$ 使 $M = IM$，则必有 $a \in R$(即上述的行列式之值)使 $aM = 0$ 且 $a \equiv 1 \pmod{I}$，若 $I \subseteq J(R)$，则 $M = 0$。

由命题 21.8(5)与定理 22.1，推论 21.3 与定理 21.1 又得

推论 22.2 设 R 为 Dedekind 环，$0 \neq I \lhd R$，则 I 为可逆 R-模，且

$$\mathrm{Cl}(R) \simeq \mathrm{Pic}(R) \simeq \{\langle I \rangle \mid 0 \neq I \lhd R\}$$

下面再给出 Dedekind 环的另两个特征刻画。

命题 22.1 设 R 为整环，则下述三点等价：

(1) R 为 Dedekind 环；

(13) $0 \neq M \in \mathrm{f.g.}\,\mathrm{P}_R\mathfrak{M} \Leftrightarrow M$ 同构于 R 的有限个非零理想的直和：

$$M \simeq \bigoplus_{j=1}^{n} I_j, \qquad 0 \neq I_j \lhd R$$

因此

$$M \simeq \bigoplus_{j=1}^{\mathrm{rank} M} M_j, \qquad M_j \text{ 为可逆 } R\text{-模}$$

(14) $\forall\, 0 \neq I \subsetneqq R$，必有惟一的一组 $M_1, \cdots, M_n \in \mathrm{Max}R$(可重复)使

$$I = M_1 M_2 \cdots M_n = M_1^{n_1} \cdots M_k^{n_k}, M_i \neq M_j,$$

$$1 \leqslant i,j \leqslant k,\ i \neq j, M_{k+1}, \cdots, M_n \in \{M_j \mid j = 1, \cdots, k\}。$$

证 由定理 22.1 的(2)，(3)，(1)等价知，这里的(1)⇔(14)。

(13)⇒(1)：由(13)知，$\forall\, 0 \neq I \lhd R$，$I \in \mathrm{P}_R\mathfrak{M}$。于是由定理 22.1 的(1)，(9)等价即得证。

(1)⇒(13)：由(1)与定理 22.1 及推论 22.2 知，(13)中"⇐"成立，现证(13)中的"⇒"。

设 $0 \neq M \in \mathrm{f.g.}\,\mathrm{P}_R\mathfrak{M}$，则可令 $M \oplus N \simeq R^n$。于是有 R-模同态的交换图

$$\begin{array}{ccc} M & \xrightarrow{\alpha} & R^n \\ & \searrow^{\pi_i\alpha} & \downarrow \pi_i \\ & & R \end{array}$$

其中 $\pi_i(x_1,\cdots,x_n)=x_i$。由 $M\neq 0$ 知必有 i 使 $\pi_i\alpha\neq 0$，记 $I=\mathrm{Im}\pi_i\alpha$，则 $0\neq I \lhd R$。但由 R 为 Dedekind 环知，I 为可逆 R-模（推论 22.2），于是 $\mathrm{rank}I=1$ 且 $I\in \mathrm{P}_R\mathfrak{M}$。于是 $\pi_i\alpha: M\twoheadrightarrow I$ 可裂。即 $M\simeq I\oplus M_1$，$M_1\in$ f. g. $\mathrm{P}_R\mathfrak{M}$ 且 $\mathrm{rank}M_1=\mathrm{rank}M-1$，依此类推即得证。 □

推论 22.3 设 R 为 Dedekind 环，$I=M_1\cdots M_n$，$M_j\in \mathrm{Max}R$，$j=1,2,\cdots,n$，则

（1）$V(I)=\{M_1,M_2,\cdots\cdots,M_n\}$，

因此，$\forall\, 0\neq I\subsetneqq R$，$|V(I)|<\infty$ 且

$$I=\prod_{M_j\in V(I)} M_j;$$

（2）R 中含 I 的理想个数是有限的。

证 （1）由设知 $I\subset M_j$，$j=1,2,\cdots,n$，因此 $M_1,M_2,\cdots,M_n\in V(I)$。

反过来，若 $M\in V(I)$，由设知 $I\neq 0$，再由定理 22.1(2)知 $M\in \mathrm{Max}R$。又由定理 22.1(4)知，必有 $I_1\lhd R$ 使 $I=MI_1$，因此 $I\subseteq I_1$。下证 $I\neq I_1$。反设 $I=I_1$ 由 I 可逆知 $R=M$ 与 $M\in \mathrm{Spec}R$ 矛盾。如果 $I_1=R$，则 $I=M$。由 Dedekind 环中理想分解的惟一性（定理 22.1(3)）知 $n=1$，$V(I)=\{M\}$。若 $I_1\neq R$，由 I_1 同样进行。由于 R 为 Noether 环，

$$I\subsetneqq I_1\subsetneqq\cdots\subsetneqq I_j\subsetneqq\cdots$$

必到有限步止，从而得到惟一分解 $I=M_1M'_2\cdots M'_n$。于是对某一个 j，$M=M_j$，故

$$V(I)=\{M_1,M_2,\cdots,M_n\}$$

（2）注意 I 可写为 $I=M_1^{n_1}\cdots M_k^{n_k}$，$M_i\neq M_j$。$R\rhd J\supseteq I$ 时，$J=M_1^{m_1}\cdots M_k^{m_k}$，$m_j\leqslant n_j$ 即得(2)。 □

命题 22.2 设 R 为 Dedekind 环，则 R 或为半局部环或为 Jacobson 半单环（域的次直积），即

（1）$J(R)\neq 0\Leftrightarrow|\mathrm{Spec}R|<\infty\Leftrightarrow|\mathrm{Max}R|<\infty\Leftrightarrow R$ 为半局部环。

（2）当 $|\mathrm{Max}R|<\infty$ 时，$R\in \mathrm{PID}$，因此

$$\mathrm{Cl}(R)\simeq \mathrm{Pic}(R)=1$$

都是平凡的，$\mathrm{K}_0(R)\simeq\mathbb{Z}$。

证 （1）只需证 $J(R)\neq 0\Leftrightarrow|\mathrm{Max}R|<\infty$，其余都是已知结果。

$J(R)\neq 0$ 时，取 $I=J(R)$，则 $V(I)=\mathrm{Max}R$。由推论 22.3 即可以知道 $|\mathrm{Max}R|<\infty$。反过来，若 $|\mathrm{Max}R|<\infty$，可令 $\mathrm{Max}R=\{M_1,M_2,\cdots,M_n\}$。于是（注意极大理想两两互素）

$$J(R)=M_1\cap M_2\cap\cdots\cap M_n=M_1M_2\cdots M_n\neq 0$$

（2）当 $|\mathrm{Max}R|<\infty$ 时，即 R 为半局部环时，可令 $\mathrm{Max}R=\{M_1,M_2,\cdots,M_n\}$。由此知

$$R/J(R)\simeq R/M_1\oplus\cdots\oplus R/M_n$$

由命题 22.1(14)知只需证每一个 M_j 都是主理想。事实上只需证 M_1 为主理想（其他的 M_j 同理可证）。

由 M_1 可逆知 $M_1^2\subsetneq M_1$（否则有 $M_1=R$，矛盾），因此有 $a\in M_1\backslash M_1^2$。于是 $aM_1^{-1}\lhd R$，但 $aM_1^{-1}\not\subset M_1$（否则有 $a\in M_1^2$，矛盾）。同理知有 $a_j\in M_1\backslash M_1M_j$，使 $a_jM_1^{-1}\not\subset M$。由上述的 $R/J(R)$ 分解式又知，可取上述的 a 使 $aM_1^{-1}\not\subset M_j$，$j=2,\cdots,n$。由此知 R 的一切极大理想都不包含 aM_1^{-1}。故 $aM_1^{-1}=R$，即 $aR=M_1$ 为主理想。 □

命题 22.2 有着有趣的应用。但(2)中的结论不可逆，比如 $\mathbb{Z}$ 为 Dedekind 环（也是 PID）$\mathbb{Z}$ 有无穷多个极大理想（$\forall$ 素数 p，$(p)=\mathbb{Z}p\in\mathrm{Max}\mathbb{Z}$）。因此不经计算即知 $J(\mathbb{Z})=0$。

由命题 22.2 又可得

推论 22.4　设 R 为 Dedekind 环且有 $0\neq I\lhd R$ 使 $1+I\subseteq R^*$，则 $J(R)\neq 0$。因此 $\mathrm{Cl}(R)\simeq\mathrm{Pic}(R)=1$ 为平凡的，$K_0(R)\simeq\mathbb{Z}$。

为研究 Dedekind 环的 K_0 群分解，先证如下引理。

引理 22.1　设 R 为 Dedekind 环，$0\neq I\subsetneq R$，则 R/I 为主理想环（PIR）（当且仅当 $I\in\mathrm{Spec}R(\mathrm{Max}R)$ 时为 PID）且为 Artin 环。

证　由命题 22.1(14)，可令

$$I=M_1^{n_1}\cdots M_k^{n_k},M_i\neq M_j,\ \forall i\neq j,\ M_j\in\mathrm{Max}R$$

由推论 22.3，又知 R 中含 I 的理想个数有限，即 R/I 中理想（都是 J/I 形，其中 $I\subset J\lhd R$）个数有限。因此对理想满足 DCC，即 R/I 为 Artin 环。又显然

$$J/I=\overline{M}_1^{m_1}\cdots\overline{M}_k^{m_k},$$

$$m_j\leqslant n_j,\ j=1,2,\cdots,k,\ \overline{M}_j\equiv M_j(\mathrm{mod}\ I)$$

于是只需再证 $\overline{M}_1$ 为主理想（其他同理可证），即证有 $y\in R$ 使 $M_1=I+yR$。

事实上仿命题 22.2(2)之证可取 $0\neq a\in M_1\backslash M_1^2$，注意 $M_1^2\not\subset M_j$，$\forall j>1$（否则，有 $M_1\subset M_j$，即 $M_1=M_j$），知 $(M_1^2,M_j)=R$，$\forall j=2,\cdots,k$. 又显然有

$(M_i,M_j)=R,j=2,\cdots,k,\ i\neq j$，故由中国剩余定理(CRT)知，有 $y\in R$ 使

$$y\equiv a(\mathrm{mod}\ M_1^2),$$
$$y\equiv 1(\mathrm{mod}\ M_j),\ j=2,\cdots,k$$

当然 $y-a\in M_1^2\subset M_1$。但 $a\in M_1\setminus M_1^2$，于是 $y\in M_1\setminus M_1^2$。注意 $I\subseteq M_1$ 即知 $I+yR\subseteq M_1$。又由 $y\equiv 1(\mathrm{mod}\ M_j),j>1$ 知 $I+yR\not\subset M_j,\forall j>1$。于是由 R 为 Dedekind 环知 $I+yR=M_1^r,r\geqslant 1$。但 $y\notin M_1^2$，于是 $r=1$，即 $I+yR=M_1$。 □

由此引理可得 Dedekind 环的一个重要性质。

推论 22.5 设 R 为 Dedekind 环，则 R 的任意理想 I 都可由 2 个元素生成，$I\neq 0$ 时，其中之一可取 I 中任意非零元(也称 I 为 $1\frac{1}{2}$生成的，或称 Dedekind 环为 $1\frac{1}{2}$-Noether 环)。

证 $\forall 0\neq a\in I,I/(a)\lhd R/(a)$，但由引理 22.1 知必有 $b\in I$ 使 $I/(a)=(b+(a))$，即 $I=(a,b)$ 由 a,b 生成。 □

推论 22.6 设 R 为 Dedekind 环，$A,B\lhd R$，则有 R-模同构 $R/B\simeq A/AB$。

证 由推论 22.5 知 $A=(a,x),a\in A,x\in R$，可取 $a\in AB\subseteq A$，作 R-模同态 $g:R\to A/AB$ 使 $g(r)=rx+AB$，则 g 为满同态。且 $\mathrm{Ker}g=\{r\in R|rx\in AB\}=\{r\in R|rA\subseteq AB\}\subseteq A^{-1}AB=B,B\subseteq\mathrm{Ker}g$ 显见。因此 $\mathrm{Ker}g=B$，故 $R/B\simeq A/AB$。 □

引理 22.2 设 R 为 Dedekind 环，$0\neq I,J\lhd R$，则有 R-模同构

$$I\oplus J\simeq R\oplus IJ$$

证 (1) 设 $I+J=R$，则有 R-模满同态

$$\alpha:I\oplus J\twoheadrightarrow R,\ (i,j)\mapsto i-j$$
$$\mathrm{Ker}\alpha=\{(i,i)|i\in I\cap J\}\simeq I\cap J=IJ(\text{因 } I+J=R)$$

由 $R\in P_R\mathfrak{M}$ 知 α 可裂，因此，$I\oplus J\simeq R\oplus IJ$。

(2) 设 $I+J\neq R$，我们来证：必有 $I_1\lhd R,I_1\simeq I\in{}_R\mathfrak{M}$ 使 $I_1+J=R$。由此即知，$J\oplus I\simeq I_1\oplus J\underset{(1)}{\simeq}R\oplus I_1J\simeq R\oplus IJ$。

事实上，任取 $0\neq a\in I$，令 $L=(aR)I^{-1}$，则 $L\lhd R$，从而 $JL\lhd R$。于是由引理 22.1 知 $R/JL\in\mathrm{PIR}$，由此知必有 $b\in L$ 使 $L=JL+bR$(注意 $L/JL\lhd R/JL$)。同乘 I 于两端得：$IL=IJL+bI$. 再以 $L=(ak)I^{-1}$代入即得 $aR=aJ+bI$。但 $0\neq a\in I\subseteq R$ 在 R 的分式域 F 内有逆元 a^{-1}。于是 $R=J+(a^{-1}b)I,a^{-1}b\in F$. 取 $I_1=(a^{-1}b)I$，则 $I_1\simeq I$ 且 $I_1+J=R$。 □

我们前面已经知道：$\forall R\in \mathrm{CRing},\mathrm{K}_0(R)\simeq\mathbb{Z}\oplus\widetilde{\mathrm{K}}_0(R)$。当 R 又为连通

环时，$K_0(R)$又有与此实质上一致的分解：$K_0(R)\simeq\mathbb{Z}\oplus rK_0(R)$。但尽管在 R 为整环时，$\mathrm{Pic}(R)\simeq \mathrm{Cl}(R)$，一般地，没有以它们为直和项的 $K_0(R)$分解式。不过，对 Dedekind 环，我们有十分满意的下述结果。

定理 22.2　设 R 为 Dedekind 环，

$$i_+ : \mathrm{Pic}(R) \to rK_0(R)$$
$$\langle M\rangle \mapsto [M]-[R]$$

则

(1) i_+ 为 Abel 群同构。因此

$$\mathrm{Pic}(R)\simeq rK_0(R)\simeq \mathrm{Cl}(R)\simeq \widetilde{K}_0(R);$$

(2) $K_0(R)$有实质上一致的 Abel 群分解

$$K_0(R)\simeq \mathbb{Z}\oplus \mathrm{Pic}(R)\simeq \mathbb{Z}\oplus \mathrm{Cl}(R)$$
$$\simeq \mathbb{Z}\oplus rK_0(R)\simeq \mathbb{Z}\oplus \widetilde{K}_0(R)$$

证　(1) 先证 i_+ 为完全确定的. 设$\langle M\rangle=\langle N\rangle\in \mathrm{Pic}(R)$，即 $M\simeq N$，则 $[M]=[N]$且 $\mathrm{rank}N=\mathrm{rank}M=1$。于是$[N]-[R]=[M]-[R]\in rK_0(R)$，即 i_+ 是完全确定的。

再证 i_+ 为群同态。由推论 22.2 知

$$\mathrm{Pic}(R)\simeq \mathrm{Cl}(R)\simeq \{\langle I\rangle \mid 0\neq I\lhd R\}$$

在 $\mathrm{Cl}(R)$中$\langle I\rangle\langle J\rangle=\langle IJ\rangle\ \forall\, I,J\lhd R$. 又由引理 22.2 知

$$I\oplus J\simeq IJ\oplus R$$

因此$[I\oplus J]=[IJ]+[R]$。于是，按 i_+ 的定义（可认为 $\mathrm{Pic}(R)=\mathrm{Cl}(R)$）

$$\begin{aligned} i_+(\langle IJ\rangle) &= [IJ]-[R]=[I\oplus J]-2[R] \\ &= ([I]-[R])+([J]-[R]) \\ &= i_+(\langle I\rangle)+i_+(\langle J\rangle) \end{aligned}$$

即 i_+ 为群同态。

$\forall\,[N]-[R^n]\in rK_0(R)$，$\mathrm{rank}N=n$. 由命题 22.1 知

$$N\simeq \bigoplus_{j=1}^{n} I_j,\qquad I_j\lhd R$$

因此

$$[N]-[R^n]=[\bigoplus_{j=1}^{n} I_j]-[R^n]=\sum_{j=1}^{n}([I_j]-[R])$$

由此知$\langle \mathrm{Im}\,i_+\rangle_{\mathbb{Z}}=rK_0(R)$，即 i_+ 为满同态。

下证 i_+ 是单的，用 §21 中的 $\det: K_0(R)\to \mathrm{Pic}(R)$，

$$\det([M]-[R])=\langle M\rangle\langle R\rangle^{-1}=\langle M\rangle$$

于是 $\det\cdot i_+=I_{\mathrm{Pic}(R)}$。因此 i_+ 为单同态，这就证出了(1)。

(2) 由(1)与过去的已知结果即得。 □

由上定理可知,计算 Dedekind 环 R 的 K_0 群,基本上归为其类数 $h=|Cl(R)|$ 的计算,$h=1\Leftrightarrow K_0(R)\simeq\mathbb{Z}\Leftrightarrow R\in$ UFD,h 为素数时 $K_0(R)\simeq\mathbb{Z}\oplus\mathbb{Z}_h$。一般地,可由 h 之值(用有限生成 Abel 群结构定理)估计出 $Cl(R)$ 的结构有几种可能性。遗憾的是 h 可能是无穷的,甚至在 1966 年 L. Claborn 已证出:任意的 Abel 群都可作为某一个 Dedekind 环的理想类群(见 Pacific J. of Math. 18(1966), 219—222)。所幸的是对代数数域 F 的代数整元环 O_F,§23 中将证明 O_F 必是 Dedekind 环,其类数 h 必是有限的(比如 §18 中提到的 n 次分圆域$\mathbb{Q}(\xi_n)$的代数整元环$\mathbb{Z}[\xi_n]$的类数必是有限的),且有一些类数公式(有的是通用的)可供应用。

注① 在代数数论中,一类最令人感兴趣的是二次域(实二次域、虚二次域),它们都可表如 $F=\mathbb{Q}(\sqrt{d})$,d 无平方因子。不难证明,在 $d\equiv2,3\pmod 4$时,$O_F=\mathbb{Z}[\sqrt{d}]$,而当 $d\equiv1\pmod 4$时,$O_F=\mathbb{Z}[\frac{1}{2}(1+\sqrt{d})]$)(下节将给出证明)。

对虚二次域($d<0$ 情况),Gauss 曾在大量计算的基础上猜测:

$$h_d=1\Leftrightarrow d=-1,-2,-3,-7,$$
$$-11,-19,-43,-67,-163(9\text{ 个数})$$

这个猜测于 1966 年为 H. Stark 证出。事实上,1934 年即已证出$|d|\to+\infty$时,$h(-d)\to+\infty$。因此对每一个类数 $k\geqslant1$,只有有限个($\mathbb{Q}\sqrt{-d}$)的 $h=k$。

对实二次域($d>0$ 情况),Gauss 也曾猜测有无穷多个 d 使 $h_d=1$. 但至今仍是一个未获解决的难题。

[Боревич, 1964]中有下列三种表可供参考。(1)$d=2$—499,h_d 的数值表;(2) 对 2000 以下(共 303 个)p,h_p 的数值表,其中 26 个素数对应类数为 3,7 个素数对应的类数为 5,4 个素数对应的类数为 7,1 个素数对应的类数为 9,1 个素数对应的类数为 11,其余 264 个素数对应的类数为 1;(3) $1\leqslant d<500$ 对应的 h_{-d}数值表(虚二次域的类数表)其中最大的类数为 32,且除 23,27,29,31 外其余的 1—32 都在表中作为类数出现。

对 $R=\mathbb{Z}[\sqrt{-d}]$形的环(由上知当$-d\equiv2,3\pmod 4$即 $d\equiv2,1\pmod 4$时为 Dedekind 环,记为 $R\in$ DD)。可用初等方法算出 $d=1,2$ 时 $h=1$,即 $R\in$ PID$\subset$DD; $d=3,7$ 时 $R\notin$ DD,但 $h=1$,而且 $K_0(R)\simeq\mathbb{Z}$;$d=5,6$ 时 $R\in$ DD,$h=2$。因此

$$K_0(\mathbb{Z}[\sqrt{-d}]) \simeq \begin{cases} \mathbb{Z}, & d = 1,2,3,7 \\ \mathbb{Z} \oplus \mathbb{Z}_2, & d = 5,6 \end{cases}$$

事实上 $\mathbb{Z}[\sqrt{-5}]$ 是第一个被发现的非 UFD 的 Dedkind 环，也是 K_0 群不同构于 $\mathbb{Z}$ 的第一个例子。

对 $R=\mathbb{Z}[\frac{1}{2}(1+\sqrt{-d})]$ 形的环，由上知当 $d\equiv 3(\mathrm{mod}\ 4)$ 时 $R\in\mathrm{DD}$。也可用初等方法具体算出(参见§23与§24)：$d=3,7,11,19$ 时，$h=1$，因此对应的 K_0 群同构于 $\mathbb{Z}$；$d=15$ 时 $h=2$；$d=23$ 时 $h=3$。因此

$$K_0(\mathbb{Z}[\frac{1}{2}(1+\sqrt{-d})]) \simeq \begin{cases} \mathbb{Z}, & d = 3,7,11,19 \\ \mathbb{Z} \oplus \mathbb{Z}_2, & d = 15 \\ \mathbb{Z} \oplus \mathbb{Z}_3, & d = 23 \end{cases}$$

有兴趣的读者可参阅[Silvester,1981]的 p. 71—p. 77。

注②　对虚二次域 $\mathbb{Q}(\sqrt{-p})$(p 为素数)，已有一些有趣的结果可供应用：

(1) 设 $p\equiv 1(\mathrm{mod}\ 8)$，则 $h_{-p}=0\ (\mathrm{mod}\ 4)$，即 $4\mid h_{-p}$(见[Боревич, 1964])；

(2) 设 $p\equiv 3(\mathrm{mod}\ 4)$，$p>3$，$V$,$R$ 分别为 $1,2,\cdots,p-1$ 中 $\mathrm{mod}\,p$ 的非平方剩余之和与平方剩余之和，则 $h_{-p}=\frac{1}{p}(V-R)$，(见[Ireland,1982])；

(3) 设 $p\equiv 3(\mathrm{mod}\ 4)$，$p>3$，$M$,$N$ 分别为 $1,2,\cdots,\frac{p-1}{2}$ 中 $\mathrm{mod}\,p$ 平方剩余的个数与非平方剩余的个数，则 h_{-p} 为奇数，且

$$h_{-p} = \begin{cases} M-N, & p \equiv 7(\mathrm{mod}\ 8) \\ \frac{1}{3}(M-N), & p \equiv 3(\mathrm{mod}\ 8) \end{cases}$$

(见[Long,1977])。

由(2)，(3)，我们可得一个更便于计算的结果：

命题 22.3　对虚二次域 $F=\mathbb{Q}(\sqrt{-p})$($p>2$ 为素数且 $p\equiv 3(\mathrm{mod}\ 4)$，其代数整元环 $O_F=\mathbb{Z}[\frac{1}{2}(1+\sqrt{-p})]$ 的类数记为 h_{-p}，令 N 为 $1,2,\cdots,\frac{p-1}{2}$ 中，$\mathrm{mod}\,p$ 的非平方剩余的个数，则 h_{-p} 为奇数，且

$$h_{-p} = \frac{p-1}{2} - \frac{2R}{p} = \begin{cases} \frac{p-1}{2} - 2N, & p \equiv 7(\mathrm{mod}\ 8) \\ \frac{1}{3}(\frac{p-1}{2} - 2N), & p \equiv 3(\mathrm{mod}\ 8) \end{cases}$$

其中

$$R=\sum_{j=1}^{\frac{p-1}{2}}(j^2(\mathrm{mod}\ p)),\ j^2(\mathrm{mod}p)\in\{1,2,\cdots,p-1\}$$

证 由于 $1+2+\cdots+(p-1)=p(p-1)/2=V+R$,因此

$$h_{-p}=\frac{1}{p}(V-R)=\frac{1}{p}\left(\frac{p(p-1)}{2}-2R\right)=\frac{p-1}{2}-\frac{2R}{p}$$

但由 $p\equiv3(\mathrm{mod}\ 4)$知 $p-1/2$ 为奇数,又由 p 为奇数知 $2R/p$ 为偶数,故 h_{-p} 为奇数。

再注意,事实上,不必检查 $1,2,\cdots,p-1$ 中那些是平方剩余。因为由

$$R=\sum_{j=1}^{\frac{p-1}{2}}(j^2(\mathrm{mod}\ p)),\ (\text{使 } j^2\mathrm{mod}p\in\{1,2,\cdots,p-1\})$$

即可得所要求的值。因此用此公式求类数极其方便。

又显然 $M+N=\frac{p-1}{2}$,即 $M=\frac{p-1}{2}-N$。因此当 $p\equiv7(\mathrm{mod}\ 8)$时

$$h_{-p}=M-N=\frac{p-1}{2}-2N$$

当 $p\equiv3(\mathrm{mod}\ 8)$时

$$h_{-p}=\frac{1}{3}(M-N)=\frac{1}{3}\left(\frac{p-1}{2}-2N\right)$$ □

由上述结果可看出研究二次域的类数当以实二次域及素数 $p\equiv5(\mathrm{mod}\ 8)$时 $\mathbb{Q}(\sqrt{-p})$的类数为重点。对素数 $p\equiv3(\mathrm{mod}\ 4)$,$p>3$ 时 $\mathbb{Q}(\sqrt{-p})$的类数(O_F 的类数也称为 F 的类数)由上述结果已可方便地算出。下面仅举一例说明。

例 1 $F=\mathbb{Q}(\sqrt{-7})$. $7\equiv3(\mathrm{mod}\ 4)$,即 $-7\equiv1(\mathrm{mod}\ 4)$, $O_F=\mathbb{Z}[\frac{1}{2}(1+\sqrt{-7})]$

$$R=1^2+2^2+3^2(\mathrm{mod}\ 7)=1+4+2=7$$

因此

$$h_{-7}=\frac{7-1}{2}-\frac{2\cdot7}{7}=3-2=1$$

即 $\mathbb{Z}[\frac{1}{2}(1+\sqrt{-7})]\in\mathrm{PID}$。

注意注①中 9 个 $h=1$ 的 d 除 $-1,-2,-3$ 外都满足 $p\equiv3(\mathrm{mod}\ 4)$,$p>3$,都可由命题 22.3 简单地算出来。计算 R 时注意以下几点可大大减轻计算量:

(1) $j^2<p$ 时即取 j^2；(2) $j^2>p$ 时 mod p 取余数 $\in[1,p-1]$；(3) 算出第一个使 $j^2>p$ 取余 a 后，在计算 $(j+1)^2 \pmod p$ 时可用由 $(j+1)^2=j^2+2j+1$ 中的 $2j+1$ 加上 a 再 mod p。当 $a<p$ 但接近 p 时可用负余数 $-b\equiv a \pmod p$ 由 $-b+2j+1 \pmod p$ 而得 a_1。再由 $a_1+(2j+1)+2 \pmod p$ 求 $(j+2)^2 \pmod p$，…，比如

例 2 $p=43,\dfrac{p-1}{2}=21$，以下"≡"都表示 mod p 运算：

$1^2=1,2^2=4,3^2=9,4^2=16,5^2=25,6^2=36$，都 <43

$7^2=49\equiv6,8^2\equiv6+2\cdot7+1=21,9^2\equiv21+17=38,10^2\equiv38+19=57\equiv14$（也可用 $10^2\equiv-5+19\equiv14$），$11^2\equiv14+21=35,12^2\equiv35+23=58\equiv15,13^2\equiv15+25=40,14^2\equiv40+27=67\equiv24,15^2\equiv24+29=53\equiv10,16^2\equiv10+31=41,17^2\equiv41+33=74\equiv31,18^2\equiv31+35=66\equiv23,19^2\equiv23+37=60\equiv17,20^2\equiv17+39=56\equiv13,21^2\equiv13+41=54\equiv11$。故求上述各式最右边的数的和得（$p$ 较大时，求 $1^2+2^2+\cdots+6^2$ 可用求和公式）

$R=1+4+9+16+25+36+6+21+38+14+35+15+40+24+10+41+31+23+17+13+11=430$

因此

$$h_{-43}=21-\frac{2\cdot430}{43}=21-20=1$$

由此知

$$K_0\left(\mathbb{Z}\left[\frac{1}{2}(1+\sqrt{-43})\right]\right)\simeq\mathbb{Z},$$

其 Cl 群，Pic 群，rK_0 群，$\widetilde{K}_0$ 群都是平凡的。

§23 二次域与二次有理函数域的类数

在本节中我们将证明：数域（$\mathbb{Q}$ 的有限次扩张域）中代数整元环都是 Dedekind 环。更一般地，特征数不为 2 的域上的有理函数域的有限次扩张域中的代数整元环也是 Dedekind 环。由上节知，对 Dedekind 环 R，$\mathrm{Cl}(R)$，$\mathrm{Pic}(R)$，$rK_0(R)$，$\widetilde{K}_0(R)$ 都是同构的。因此其类数计算的重要性以及对确定 $K_0(R)$ 的意义是显见的。特别是二次域 $\mathbb{Q}(\sqrt{d})$（d 无平方因子，$d>0$ 时称为实二次域，$d<0$ 时称为虚二次域，其代数整元环的类数也常被称为此域的类数）的类数计算，因多年来一直是代数数论中活跃的热门课题之一，

我们将作比较详尽的介绍。

设 Q 为域，$\mathrm{Ch}Q\neq 2$，F 为 Q 的二次扩张域，当 $Q=\mathbb{Q}$ 时，$F=\mathbb{Q}(\sqrt{d})$（$\mathbb{Z}[\sqrt{d}]$的分式域），$d\in\mathbb{Z}$. 当 $Q=K(X)$ 为域 K 上的有理函数域（当然 $\mathrm{Ch}K\neq 2$）时，$F=Q(\sqrt{d})$ 为其子环 $Z[\sqrt{d}]$的分式域。其中 $d\in K[X]$，$Z=K[X]$。于是我们使用记号

$$Z=\begin{cases}\mathbb{Z}, & Q=\mathbb{Q}\\ K[X], & Q=K(X),\mathrm{Ch}K\neq 2\end{cases}$$

显然，$Z\in\mathrm{PID}$，且 $\forall a\in F$，a 可惟一地表为 $a=x_0+x_1\sqrt{d}$，$x_0,x_1\in Q$（$\forall a\in Z[\sqrt{d}]$，a 可惟一地表作上面的形式，其中 $x_0,x_1\in Z$），记

$$\bar{a}=x_0-x_1\sqrt{d}$$

称为 a 在 F 中的**共轭元**(conjugate)。称

$$T(a)\equiv\mathrm{tr}(a)=a+\bar{a}=2x_0$$

为 a 的**迹**(trace)。并称

$$N(a)=a\bar{a}=x_0^2-dx_1^2$$

为 a 的**范**(norm)。更一般地，若 F 为 Q 的 n 次扩张域（Q 添加一个 $Q[x]$中 n 次首一既约多项式 $f(x)$的根 α 所得），则 F 为 n 维的 Q-线性空间。任取其基 $\alpha_1,\alpha_2,\cdots,\alpha_n$，则 $\forall a\in F$，$a(\alpha_1\alpha_2\cdots\alpha_n)^T=A(\alpha_1\alpha_2\cdots\alpha_n)^T$，$A\in F^{n\times n}$。称 A 的迹（对角元之和）为 a 的**迹**，称 $\det A$ 为 a 的**范**。它们都与基的选取无关。显然有

引理 23.1 在上述记号下，

(1) “-”（使 $a\mapsto\bar{a}$）为 F 的环自同构；

(2) $\bar{a}=a\Leftrightarrow a\in Q$；

(3) $T(a+b)=T(a)+T(b)$，

$$T(qa)=qT(a),\ \forall a,b\in F,\ q\in Q;$$

(4) $N(ab)=N(a)N(b)$，

$$N(qa)=q^nN(a),\ \forall a,b\in F,\ q\in Q,\ n=[F:Q];$$

(5) F/Q 为可分扩张（比如 $\mathrm{Ch}Q=0$ 时）$\Leftrightarrow T\neq 0$；

(6) $\alpha\in F$ 在 Q 上的极小多项式为 $f(x)=x^n+a_1x^{n-1}+\cdots+a_{n-1}x+a_n$ 时，$T(\alpha)=-a_1$，$N(\alpha)=(-1)^na_n$。

设 $a\in F\backslash Q$，记

$$f_a(X)=X^2-T(a)X+N(a)\in Q[X]$$

则 $f_a(X)$为 a 的极小多项式。F 的代数整元环记为 O_F，则

$$O_F=\{a\in F\mid 有首一多项式\ f(X)\in Z[X]\ 使\ f(a)=0\}。$$

下面来证部分已用过但未加证明的下述引理。

引理 23.2　设 F 为 Q 的二次扩张，$\mathrm{Ch}Q\neq 2$。

(1) 当 $Q=K(X)$，$\mathrm{Ch}K\neq 2$ 时，$O_F=Z[\sqrt{d}]=K[X][\sqrt{d}]$，$d\in Z$ 无平方因子；

(2) $Q=\mathbb{Q}$，$F=\mathbb{Q}(\sqrt{d})$，d 无平方因子，$d\in\mathbb{Z}$，时

$$O_F=\begin{cases}\mathbb{Z}[\sqrt{d}],d\equiv 2,3(\bmod 4)\\ \mathbb{Z}[\frac{1}{2}(1+\sqrt{d})],d\equiv 1(\bmod 4)\end{cases}$$

证　(1) $Z[\sqrt{d}]\subset O_F$ 是显见的。又

$\forall a=x_0+x_1\sqrt{d}\in O_F$，则有首一多项式 $f(X)\in Z[X]$ 使 $f(a)=0$。当 $\deg f(X)=1$ 时显然 $a\in Z$，当 $\deg f(X)>1$ 时，必然 $\deg f(X)=2$，即 $f(X)=X^2-T(a)X+N(a)$，其中 $T(a)=2x_0\in Z$，$N(a)=x_0^2-dx_1^2\in Z$，而 $Z=K[X]$。由 $\mathrm{Ch}K\neq 2$ 知 $x_0\in Z$，$dx_1^2\in Z$。但 $Z=K[X]\in\mathrm{PID}\subset\mathrm{UFD}$，$d\in Z$ 无平方因子，$x_1^2\in Q$，因此 $x_1\in Z$，即 $a\in Z[\sqrt{d}]$，由此即知 $O_F=Z[\sqrt{d}]$。

(2) 注意 $\mathbb{Z}[\sqrt{d}]\subseteq\mathbb{Z}[\frac{1}{2}(1+\sqrt{d})]$。

$\mathbb{Z}[\sqrt{d}]\subseteq O_F$ 是显见的. 同时 $d\equiv 1(\bmod 4)$时，由于$\frac{1}{2}(1+\sqrt{d})$的极小多项式为 $X^2-X+\frac{1-d}{4}\in\mathbb{Z}[X]$，此时$\mathbb{Z}[\frac{1}{2}(1+\sqrt{d})]\subseteq O_F$ 也是显见的。

另一方面，由于$\forall a=x_0+x_1\sqrt{d}\in O_F$，其中 $x_0,x_1\in\mathbb{Q}$，而 $T(a)$，$N(a)\in\mathbb{Z}$。当 $x_0\in\mathbb{Z}$ 时由 $x_0^2-dx_1^2\in\mathbb{Z}$，知 $dx_1^2\in\mathbb{Z}$。仿(1)之证知 $x_1\in\mathbb{Z}$，于是 $a\in\mathbb{Z}[\sqrt{d}]\subseteq\mathbb{Z}[\frac{1}{2}(1+\sqrt{d})]$。当 $x_0\notin\mathbb{Z}$ 时，由 $T(a)=2x_0\in\mathbb{Z}$ 知，令 $y_0=2x_0$，$y_1=2x_1$，则 $y_0\equiv 1(\bmod 2)$。于是 $y_0^2\equiv 1(\bmod 4)$，又由 $y_0^2-dy_1^2=N(2a)=4N(a)\in 4\mathbb{Z}$ 知 $dy_1^2\in\mathbb{Z}$，仿上知 $y_1\in\mathbb{Z}$。而由 $y_0^2-dy_1^2\in 4\mathbb{Z}$ 与 $y_0^2\equiv 1(\bmod 4)$又知 $dy_1^2\equiv 1\ (\bmod 4)$。于是 $y_1\equiv 1(\bmod 2)$，$y_1^2\equiv 1(\bmod 4)$。由此即知 $d\equiv 1(\bmod 4)$。因此 $d\equiv 2,3(\bmod 4)$时 $O_F=\mathbb{Z}[\sqrt{d}]$。当 $d\equiv 1(\bmod 4)$时，取 $b=\frac{1}{2}(1+\sqrt{d})$。又 $a=x_0+x_1\sqrt{d}\in O_F$，$x_0\in\mathbb{Z}$ 时 $a\in\mathbb{Z}[\sqrt{d}]$；$x_0\notin\mathbb{Z}$ 时 $a=\frac{1}{2}(y_0+y_1\sqrt{d})$，$y_0\equiv y_1\equiv 1(\bmod 2)$，此时 $a-b\in\mathbb{Z}[\frac{1}{2}(1+\sqrt{d})]$，因此 $a\in\mathbb{Z}[\frac{1}{2}(1+\sqrt{d})]$。于是 $d\equiv 1(\bmod 4)$时，$O_F=\mathbb{Z}[\frac{1}{2}(1+\sqrt{d})]$。　□

下面来证明

定理 23.1 （1）设 K 为域，$\mathrm{Ch}K\neq 2$，$Q=K(X)$为有理函数域，而 $F=Q(\sqrt{d})$，$d\in K[X]=Z$ 无平方因子，则 $\mathrm{O_F}=Z[\sqrt{d}]$为 Dedekind 环；

（2）设 $F=\mathbb{Q}(\sqrt{d})$，$d\in\mathbb{Z}$ 无平方因子，则 $\mathrm{O_F}$ 为 Dedekind 环；

（3）设$[F:Q]=n$，则 $\mathrm{O_F}=\{a\in F\mid$ 有首一多项式 $f(x)\in\mathbb{Z}[x]$使 $f(a)=0\}$为 Dedekind 环。

证 （1）由 $Z=K[X]$为 Noether 环，$\mathrm{O_F}\in \mathrm{f.g.}_Z\mathfrak{M}$ 知 $\mathrm{O_F}$ 为 Noether（整）环。

$\forall 0\neq P\in\mathrm{Spec}\mathrm{O_F}$，再来证 $P\in\mathrm{Max}\mathrm{O_F}$。

事实上，$0\neq Z\cap P\in\mathrm{Spec}Z$，而 $Z=K[X]\in\mathrm{PID}$ 为 Dedekind 环，因此 $Z\cap P\in\mathrm{Max}Z$，即 $Z/Z\cap P$ 为域。作标准同态

$$g:Z\to \mathrm{O_F}/P$$
$$z\mapsto \bar{z}\equiv z(\mathrm{mod}\ P)$$

则 $\mathrm{Ker}g=Z\cap P$。于是

$$Z/Z\cap P\simeq\bar{Z}\equiv Z(\mathrm{mod}\ P)<\mathrm{O_F}/P$$

由此知，$\mathrm{O_F}/P$ 为域 $Z/Z\cap P$ 上的有限维线性空间。因此 $\forall 0\neq a\in\mathrm{O_F}/P$，必有最小的 k 使

$$y_0+y_1a+\cdots+y_ka^k=0,$$
$$y_j\in Z/Z\cap P,\ j=1,2,\cdots,k,y_k\neq 0,y_0\neq 0$$

但 $y_0\neq 0$ 在域 $Z/Z\cap P$ 中可逆，而

$$a(y_1+\cdots+y_ka^{k-1})=-y_0$$

因此 a 可逆（在 $\mathrm{O_F}/P$ 中），即 $\mathrm{O_F}/P$ 为域，因此 $P\in\mathrm{Max}\mathrm{O_F}$。

再来证 $\mathrm{O_F}$ 的整闭性。注意 F 为 $\mathrm{O_F}$ 的分式域，任取 $a\in F$ 为 $\mathrm{O_F}$-整元来证$a\in\mathrm{O_F}$ 即可。事实上由 a 为 $\mathrm{O_F}$-整元知有 $a_j\in\mathrm{O_F}$，$j=1,2,\cdots,n$，使

$$a^n+a_1a^{n-1}+\cdots+a_n=0$$

因此由 $\mathrm{O_F}\in\mathrm{f.g.}_Z\mathfrak{M}$ 知 $\mathrm{O_F}[a]\in\mathrm{f.g.}_Z\mathfrak{M}$。不妨令

$$\mathrm{O_F}[a]=Zb_1+\cdots+Zb_m,\ b_j\in\mathrm{O_F},$$
$$ab_i=a_{i1}b_1+\cdots+a_{im}b_m,\ i=1,2,\cdots,m,a_{ij}\in Z。$$

于是记 $A=(a_{ij})\in Z^{m\times m}$。有

$$(aI_m-A)(b_1,\cdots,b_m)^T=0$$

但 $\mathrm{O_F}$ 为整环。因此 $\det(aI_m-A)=0$，即 a 为 Z-整的。因此 $a\in\mathrm{O_F}$。故由定理 22.1(11)知 $\mathrm{O_F}$ 为 Dedekind 环。

用上述方法同理可证(2)，(3)。 □

在(1)，(2)的情况下，任取素元素 $p\in Z$，注意 Z/pZ 为域，

$$\{J \lhd O_F \mid pO_F \subset J\} \underset{1-1}{\leftrightarrow} \{\bar{J} \lhd O_F/pO_F\}$$

且 O_F/pO_F 为域 Z/pZ 上维数≤2 的线性空间，$\bar{J}=J/pO_F$ 为其子空间。我们可以断言：$pO_F \lhd O_F$ 不能有 3 个或更多的可重复素因子(即极大素因子，因为 O_F 为 Dedekind 环)。因此若 $M_j \supseteq pO_F$，$j=1,2,3$，$M_j \in \mathrm{Max}O_F$，则

$$pO_F \subseteq M_1M_2M_3 \subsetneqq M_1M_2 \subsetneqq M_1 \subsetneqq O_F$$

于是有 Z/pZ 上线性空间(≤2 维)包含关系

$$0 \neq O_F/pO_F \supsetneqq M_1/pO_F \supsetneqq M_1M_2/pO_F \supsetneqq M_1M_2M_3/pO_F$$

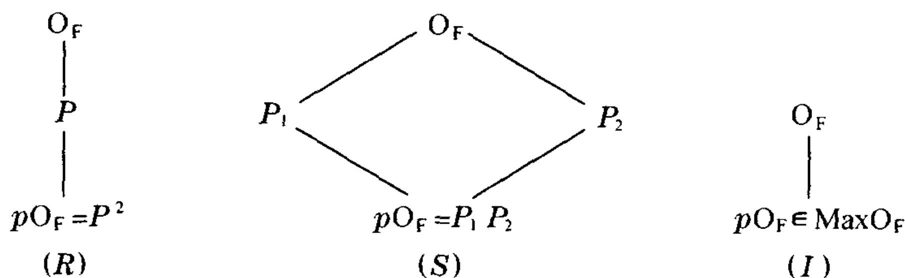
这不可能。于是，我们可得(下面诸图中，线下方的为线上方的子 O_F-模)。

命题 23.1　设 Q 为域，F 为 Q 的二次扩张域，$Z=\mathbb{Z}$($Q=\mathbb{Q}$ 时)或 $K[X]$($Q=K(X)$，$\mathrm{Ch}K\neq 2$ 时)，O_F 为 F 的代数整元环，素元 $p\in Z$，则恰有三种可能：

(R) 恰有一个 $P\in \mathrm{Spec}O_F(\mathrm{Max}O_F)$严格包含着 pO_F(因此 $P^2 \mid pO_F$)．此时称 p 在 O_F(或 F)中是**分歧的**(ramified)，称 P 为 p 上惟一的素理想，常记为 $\hat{p}$。此时 $pO_F=P^2$ 且 $\bar{P}\equiv P(\mathrm{mod}\ pO_F)=J(O_F/pO_F)$；

(S) 恰有两个不同的 $P_1,P_2\in \mathrm{Spec}O_F(\mathrm{Max}O_F)$严格包含 pO_F(即 pO_F 无平方素理想因子)，此时称 p 在 O_F(或 F)中是**分裂的**(split)。在此情况下，$O_F/pO_F\simeq F_1\oplus F_2$，$F_j\simeq Z/pZ$ 为域；

(I) $pO_F\in \mathrm{Spec}O_F(\mathrm{Max}O_F)$，因此 O_F 中无其他素理想包含 pO_F，此时称 p 在 O_F(或 F)中是**惯性的**(inert)。在此情况下，$O_F/pO_F\simeq \mathbb{F}_{p^2}$ 为 Z/pZ 的二次扩张域。



一般地，设 F 为域 Q 的 n 次(代数)扩张域，$\beta_1,\beta_2,\cdots,\beta_n\in F$，记

$$\Delta(\beta_1,\beta_2,\cdots,\beta_n)=\det(T(\beta_i\beta_j)),$$

称为 $\beta_1,\beta_2,\cdots,\beta_n$ 的**判别式**(discriminant)，可证 $\Delta(\beta_1,\beta_2,\cdots,\beta_n)\neq 0$ 时 β_1，$\beta_2,\cdots,\beta_n$ 必为 F 在 Q 上的基。在 F 为 Q 的可分扩张时，二者是等价的(反过来也成立)。这里，F 为 Q 的可分扩张是指 F 的任一元素 α 都是可分的，即有 $f(x)\in Q[x]$，$f(x)$无重根，使 $f(\alpha)=0$。完全域(指其上的不可约多项式都无重根，比如特征数为 0 的域，有限域等都是完全域)的代数扩张都

是可分扩张。对 Q 的可分扩张 F,

$$\Delta(\beta_1,\beta_2,\cdots,\beta_n) = \det(\beta_i^{(j)})^2,$$

其中 $\beta_i=\beta_i^{(1)},\beta_i^{(2)},\cdots,\beta_i^{(n)}$ 为 β_i 在 Q 上的全体共轭元。而

$$\Delta(1,\beta,\cdots,\beta^{n-1}) = (-1)^{n(n-1)/2}N(f'(\beta)),$$

其中 $f(x)\in Q[x]$ 为 β 的极小多项式。又当 $Q=\mathbb{Q}$ 且 $\beta_1,\cdots,\beta_n\in O_F$ 时,$\Delta(\beta_1,\beta_2,\cdots,\beta_n)\in\mathbb{Z}$。于是 F 在 $\mathbb{Q}$ 上的基中必有使 $|\Delta(\beta_1,\beta_2,\cdots,\beta_n)|$ 取最小值的基 $\beta_1,\beta_2,\cdots,\beta_n$。对这种基,在引理 7.3 中我们已得如下结果:设 $[F:Q]=n$,O_F 为 F 中的代数整元环,$0\neq A\lhd O_F$,若 $\alpha_1,\alpha_2,\cdots,\alpha_n\in A$ 为 F 在 $\mathbb{Q}$ 上的基且使 $|\Delta(\alpha_1,\alpha_2,\cdots,\alpha_n)|$ 最小,则 $A=\mathbb{Z}\alpha_1+\mathbb{Z}\alpha_2+\cdots+\mathbb{Z}\alpha_n$,称 $\alpha_1,\alpha_2,\cdots,\alpha_n$ 为 A 的**整基**,它总是存在的。

由此知 $F=\mathbb{Q}(\sqrt{d})$ 时,O_F 必有整基 w_1,w_2,即 O_F 有惟一表示:$O_F=\mathbb{Z}w_1+\mathbb{Z}w_2$. 当 $d\equiv2,3 \pmod 4$ 时可取 $w_1=1,w_2=\sqrt{d}$;$d\equiv1\pmod 4$ 时可取 $w_1=1,w_2=\dfrac{-1+\sqrt{d}}{2}$。于是易算这些基的判别式(记为 $\Delta(\sqrt{d})$ 或 Δ)

$$\Delta(\sqrt{d}) = \begin{cases}4d, & d\equiv 2,3 \pmod 4\\ d, & d\equiv 1 \pmod 4\end{cases}$$

用 Legendre 记号

$$\left(\frac{m}{p}\right)=\begin{cases}1, & m \text{ 为 mod } p \text{ 平方剩余,即 } x^2\equiv m \pmod p \text{ 有整解}\\ -1, & m \text{ 为 mod } p \text{ 非平方剩余,即 } x^2\equiv m (\text{mod}) \text{ 无整解}\\ 0, & p\mid m\end{cases}$$

可证:对素数 $p>2$,$\left(\frac{\Delta}{p}\right)=-1$(即 $\left(\frac{d}{p}\right)=-1$)时,$pO_F\in \mathrm{Max}O_F$;$\left(\frac{\Delta}{p}\right)=1$(即 $\left(\frac{d}{p}\right)=1$)时,$pO_F=P_1P_2$,其中 $P_1=(p,a+\sqrt{\Delta})$,$P_2=(p,-a+\sqrt{\Delta})$,$P_1,P_2\in\mathrm{Spec}O_F$,$\pm a$ 为 $x^2\equiv\Delta\pmod p$ 之解;而 $\frac{\Delta}{p}=0$(即 $\left(\frac{d}{p}\right)=0$)时,$pO_F=(p,\sqrt{\Delta})^2$,$P=(p,\sqrt{\Delta})\in\mathrm{Spec}O_F$. 对于素数 2,当 $d\equiv5\pmod 8$ 时,$2O_F\in\mathrm{Spec}O_F$;当 $d\equiv1\pmod 8$ 时,$2O_F=(2,(1+\sqrt{d})/2)(2,(1-\sqrt{d})/2)$ 为 O_F 中两个不同的素理想之积;当 $d\equiv2\pmod 4$ 即 $d\equiv2,6\pmod 8$ 时,$2O_F=(2,\sqrt{d})^2$ 为 O_F 中素理想 P 的平方,而当 $d\equiv3\pmod 4$ 即 $d\equiv3,7\pmod 8$ 时,$2O_F=(2,1+\sqrt{d})^2$ 仍是 O_F 中素理想 $P=(2,1+\sqrt{d})$ 的平方。因此可列出下表(见[Berrick,2000])。

素数 p	2	素数 $p>2$		
		$(\frac{d}{p})=0$,即 $p\mid d$	$(\frac{d}{p})=1$	$(\frac{d}{p})=-1$
$d\equiv 2,3(\mathrm{mod}\ 4)$	R	R	S	I
$d\equiv 1(\mathrm{mod}\ 8)$	S	R	S	I
$d\equiv 5(\mathrm{mod}\ 8)$	I	R	S	I
		O_F/pO_F 有幂零元	$O_F/pO_F\simeq\mathbb{F}_p\oplus\mathbb{F}_p$	$O_F/pO_F=\mathbb{F}_{p^2}$

下面我们来证更一般的结果。

命题 23.2　(1) 设 K 为域,$\mathrm{Ch}K\neq 2$,$Q=K(X)$,$F=Q(\sqrt{d})$,并且 $d\in Z=K[X]$ 无平方因子,$p\in Z$ 为素元;或 $Q=\mathbb{Q}$,$Z=\mathbb{Z}$ 但 $d\not\equiv 1(\mathrm{mod}\ 4)$ 无平方因子,则 $O_F=Z[\sqrt{d}]$ 且

(i) 若 $d\not\equiv a^2(\mathrm{mod}\ p)$, $\forall a\in Z/pZ$,则 p 是惯性的;

(ii) 若 $Y^2-d\equiv 0(\mathrm{mod}\ p)$ 有两个不同的解 ε 与 $-\varepsilon$(即 $d\equiv\varepsilon^2(\mathrm{mod}\ p)$ 且 $p\neq 2$),则 p 是分裂的,且 pO_F 的素因子为 $P_1=(p,\sqrt{d}-e)$,$P_2=(p,\sqrt{d}+e)$,其中 $\bar{e}\equiv\varepsilon(\mathrm{mod}\ p)$;

(iii) $p=2$ 是分歧的,且 $d\equiv 2(\mathrm{mod}\ 4)$ 时,$\hat{2}=(2,\sqrt{d})$,且 $d\equiv 3(\mathrm{mod}\ 4)$ 时,$\hat{2}=(2,1+\sqrt{d})$;

(iv) $p\mid d$ 时,p 为分歧的,且 $\hat{p}=(p,\sqrt{d})$。

(2) $Q=\mathbb{Q}$ 且 $d\equiv 1(\mathrm{mod}\ 4)$ 时,$O_F=\mathbb{Z}[\frac{1}{2}(1+\sqrt{d})]$ 且

(v) $2\nmid p$ 时,(1)中的(i),(ii),(iv)成立;

(vi) 设 $p=2$,则

① $d\equiv 1(\mathrm{mod}\ 8)$ 时,2 是分裂的,$2O_F$ 的素因子为 $P_1=(2,(1+\sqrt{d})/2)$,$P_2=(2,(1-\sqrt{d})/2)$;

② $d\equiv 5(\mathrm{mod}\ 8)$ 时,2 是惯性的,即 $2O_F\in\mathrm{Max}O_F$。

证　(1) 由引理 23.2 知 $O_F=Z[\sqrt{d}]$,于是

$$O_F/pO_F\simeq(Z/pZ)[Y]/(Y^2-\bar{d}),\ \bar{d}\ 为同余类\ d(\mathrm{mod}\ p)。$$

(i) 当 $d\not\equiv a^2(\mathrm{mod}\ p)$, $\forall a\in Z/pZ$ 时,$Y^2-\bar{d}$ 既约。因此 O_F/pO_F 为域,即 $pO_F\in\mathrm{Max}O_F$。因此 p 为惯性的。

(ii) $Y^2-d\equiv 0(\mathrm{mod}\ p)$ 有不同的二解 $\pm\varepsilon(p\neq 2)$ 时,

$$Y^2-\bar{d}=(Y-\varepsilon)(Y+\varepsilon)$$

因此,由中国剩余定理(CRT)知,

$$O_F/pO_F \simeq Z/pZ \oplus Z/pZ$$

为二域之直积。于是 p 为分裂的，且含 p 的素理想恰为 $P_1=(p,\sqrt{d}-e)$，$P_2=(p,\sqrt{d}+e)$，其中 $\bar{e}=\varepsilon$。

当 $Y^2-d\equiv 0 \pmod p$ 有重根 $\varepsilon\in Z/pZ$ 时，对 Y 取导数知 $2\varepsilon=0$，于是 $\varepsilon=-\varepsilon,\varepsilon^2=-\varepsilon^2=-\bar{d}$，因此 $2d\equiv 0 \pmod p$，即 $p|2d$，因此 $p=2$ 或 $p|d$。

$p=2$ 时，$Z/2Z=\{\bar{0},\bar{1}\}$，$\forall d\in Z$，或 $Y^2-\bar{d}=Y^2$（$d\equiv 2 \pmod 4$ 时），或 $Y^2-\bar{d}=Y^2-\bar{1}=(Y-\bar{1})^2$（$d\equiv 3 \pmod 4$ 时），此时 $O_F/2O_F$ 有非零幂零元。因此不是域，也不是两域之直和。此时可肯定 2 是分歧的，且在 $d\equiv 2 \pmod 4$ 时，$\hat{2}=(2,\sqrt{d})$；$d\equiv 3 \pmod 4$ 时 $\hat{2}=(2,1+\sqrt{d})$。于是(iii)成立。

(iv) $p|d$ 时 $\bar{d}=\bar{0}$，因此

$$O_F/pO_F \simeq (Z/pZ)[Y]/Y^2$$

有非零幂零元，因此不是域也不是两域之直积。于是 p 为分歧的且 $\hat{p}=(p,\sqrt{d})$。

(2) 下面只需考察 $Q=\mathbb{Q},p=2\in\mathbb{Z}$ 且 $d\equiv 1 \pmod 4$（即(vi)）的情况，此时由引理 23.2 知，$O_F=\mathbb{Z}[\frac{1}{2}(1+\sqrt{d})]$ 且 $\frac{1}{2}(1+\sqrt{d})$ 有极小多项式 $Y^2-Y+(1-d)/4$（二根为 $\frac{1\pm\sqrt{d}}{2}$）。于是

$$O_F/2O_F = (\mathbb{Z}/2\mathbb{Z})[Y]/(Y^2-Y+\overline{(1-d)/4})$$

又可分为两种情况：

① $d\equiv 1 \pmod 8$，此时必有 $4|(1-d)$，且 $\overline{(1-d)/4}=\bar{0} \pmod 2$，于是上述的极小多项式为 $Y^2-Y=Y(Y-\bar{1})$。由此知 2 为分裂的。此时 2 的两个素因子为 $P_1=(2,(1+\sqrt{d})/2)$ 与

$P_2=(2,1+(1+\sqrt{d})/2)=(2,(1-\sqrt{d})/2)$；

② $d\equiv 5 \pmod 8$ 时，上述的极小多项式为 $Y^2-Y-\bar{1}$，它在 $\mathbb{Z}/2\mathbb{Z}$ 上是既约的。于是 2 为惯性的，即 $2O_F\in \mathrm{Max}O_F$。 □

在引理 7.4 中对 $A\lhd O_F$ 曾定义 $\|A\|=|O_F/A|$ 为理想 A 的范(norm)。注意 $\forall a\in O_F$，a 的范 $N(a)$ 未必为正数（如 $O_F=\mathbb{Z}[\sqrt{3}]$，$a=1+2\sqrt{3}$，$N(a)=1^2-3\cdot 2^2=-11<0$）。但对理想的范，我们可得如下结果。

命题 23.3 设 O_F 为（实、虚）二次域 F 中的代数整元环，$0\neq P\in \mathrm{Spec}O_F$，则 $P\cap\mathbb{Z}=p\mathbb{Z}$，$p$ 为素数且

(1) $\|P\|=\begin{cases} p, & p \text{ 为分歧或分裂的（记为 } p\in R\cup S) \\ p^2, & p \text{ 为惯性的（记为 } p\in I) \end{cases}$

(2) $\forall A \lhd O_F$，$\|A\| \geqslant 0$ 且仅当 $A=O_F$ 时 $\|A\|=0$；

(3) $\forall A,B \lhd O_F$，$\|AB\|=\|A\|\cdot\|B\|$；

(4) $\|aO_F\|=|N(a)|$，$\forall a\in O_F$。

证　注意 $P\cap\mathbb{Z}\lhd\mathbb{Z}$ 且 $\mathbb{Z}\in$ PID 即知 $P\cap\mathbb{Z}=p\mathbb{Z}$，$p\in\mathbb{Z}$。显然，$p\mathbb{Z}\in \mathrm{Spec}\mathbb{Z}$，因而 p 为素数。由 O_F 为 Dedekind 环知，$P\in \mathrm{Max}O_F$，于是 O_F/P 为域。因此，此域为 $\mathbb{Z}_p=\mathbb{Z}/p\mathbb{Z}$ 的 1 次或 2 次扩张，即 $\|P\|=p$ 或 p^2。但 $O_F/P\simeq(O_F/pO_F)/(P/pO_F)$，$O_F/pO_F$ 为 $\mathbb{Z}_p$ 上的 2 维线性空间。当 p 分歧时，$P=\hat{p}$，P/pO_F 为 O_F/pO_F 的 1 维子空间。当 p 分裂时 $P=P_1$ 或 P_2，此时 P/pO_F 也是 O_F/pO_F 的 1 维子空间。因此 $\|P\|=p$，p 为惯性的时 $P=pO_F$，$\|P\|=p^2$，于是结论(1)成立。

(2) 是显见的。

(3) 由 O_F-模正合列

$$0\to A/AB\to O_F/AB\to O_F/A\to 0$$

及同构 $A/AB\simeq O_F/B$（推论 22.6）即得(3)。

(4) 对 a 的共轭元 $\bar{a}$，由 $aO_F\simeq\bar{a}O_F$ 知 $\|aO_F\|=\|\bar{a}O_F\|$。于是

$$\begin{aligned}\|aO_F\|^2&=\|aO_F\cdot\bar{a}O_F\|=\|a\bar{a}O_F\|\\&=\|N(a)O_F\|=\|\,|N(a)|\,O_F\|\end{aligned}$$

将 $|N(a)|\in\mathbb{N}$ 分解为素数之积。注意对素数 p，O_F/pO_F 为 $\mathbb{Z}_p$ 上的 2 维线性空间，因此 $\|pO_F\|=p^2$。由此即知 $\|aO_F\|^2=N(a)^2$，于是有 $\|aO_F\|=|N(a)|$。 □

由此命题并注意到 O_F 的理想都是素理想之积，以及任意正数 n 的惟一分解 $n=p_1^{n_1}p_2^{n_2}\cdots p_k^{n_k}$（$p_1,p_2,\cdots,p_k$ 为互异素数），立得

推论 23.1　设 O_F 为二次域 F 中的代数整元环，则对任意的正整数 n，O_F 中范为 n 的理想个数有限。因此，范不超过 n 的理想个数也有限。

下面我们来证：任意数域 F 的代数整元环的类数 h_F 也都是有限的。（虽然过去我们已提过这个结果，鉴于此结果对 K_0 群研究有重要意义，我们在此仍给出证明）。

先证 A. Hurwitz 关于 Euclid 算法推广的一个结果：

引理 23.3　设 F 为数域，$[F:\mathbb{Q}]=n$，O_F 为 F 中的代数整元环，则有由 F 确定的正整数 m，使对 $\forall\alpha,\beta\in O_F$，$\beta\neq 0$，有 t，$1\leqslant t\leqslant m$，与 $w\in O_F$ 满足

$$|N(t\alpha-w\beta)|<|N(\beta)|$$

证　记 F 中的元素 $\gamma=\alpha/\beta$，只需证有 $m>0$ 与 $w\in O_F$，$1\leqslant t\leqslant m$，可使 $|N(t\gamma-w)|<1$。为此取 $w_1,\cdots,w_n$ 为 O_F 的整基，则有表示式

$$\gamma = \sum_{j=1}^{n} \gamma_j w_j, \ \gamma_j \in \mathbb{Q},$$

$$| N(\gamma) | = \left| \prod_{j=1}^{n} \left(\sum_{i=1}^{n} \gamma_i w_i^{(j)} \right) \right|$$

$$\leqslant C(\max_{1 \leqslant i \leqslant n} | \gamma_i |)^n, \text{ 其中 } C \equiv \prod_{j=1}^{n} \left(\sum_{i=1}^{n} | w_i^{(j)} | \right) > 0,$$

这里 $w_i^{(j)}$ 为 w_i 的共轭元。令 $m=b^n>C$(即 $b>\sqrt[n]{C}$)，且记 $\gamma_j=a_j+b_j$. 其中 $b_j=\{\gamma_j\}$(γ_j 的分数部分)，于是 $0\leqslant b_j<1$，$a_j=[\gamma_j]$(不超过 γ_j 的最大整数)，并记

$$[\gamma] = \sum_{j=1}^{n} a_j w_j, \ \{\gamma\} = \sum_{j=1}^{n} b_j w_j$$

则 $[\gamma]+\{\gamma\}=\gamma$ 且 $[\gamma]\in O_F$，作

$$\varphi: F \to \mathbb{R}^n$$

$$\sum_{j=1}^{n} \gamma_j w_j \mapsto (\gamma_1, \cdots, \gamma_n)$$

则 $\varphi(\{\gamma\})\subset[0,1)\times\cdots\times[0,1)\equiv V$(边长为 1 的 n 维(开)立方体)。对 $1\leqslant k\leqslant b^n+1=m+1$。考察 $\varphi(\{k\gamma\})$，由抽屉原则知，至少有两个(比如 $\varphi(\{h\gamma\})$ 与 $\varphi(\{l\gamma\})$，$h>l$)属同一个小立方体(边长为 $\frac{1}{b}$)。令 $t=h-l$，则 $1\leqslant t\leqslant b^n=m$，取 $t\gamma=w+\delta$，$w=[t\gamma]\in O_F$，δ 的坐标(在基 $w_1,\cdots,w_n$ 下)的绝对值都 $\leqslant\frac{1}{b}$。于是

$$N(t\gamma - w) = N(\delta) \leqslant C\left(\frac{1}{b}\right)^n = C/b^n < 1 \qquad \square$$

由此引理可证

定理 23.2 (H. Minkowski) 设 F 为数域，则 F 的代数整元环 O_F 的类数 $h_F\equiv|\mathrm{Cl}(O_F)|<\infty$。因此 K_0O_F 为有限生成 Abel 群。

证 $\forall\, 0\neq A\lhd O_F$，$0\neq\alpha\in A$，则 $|N(\alpha)|$ 为正整数，因此有 $0\neq\beta\in A$ 使

$$| N(\beta) | = \min\{ | N(\alpha) | \mid 0 \neq \alpha \in A\}$$

由引理 23.3 知，$\forall\,\alpha\in A$，必有 t 与 m，$1\leqslant t\leqslant m$，以及 $w\in O_F$ 使

$$| N(t\alpha - w\beta) | < | N(\beta) |$$

由 $t\alpha-w\beta\in A$ 与 $|N(\beta)|$ 的最小性即知 $t\alpha-w\beta=0$。即 $t\alpha\in\beta O_F$，因此 $m!A\subset\beta O_F$。令 $B=\frac{1}{\beta}m!A$，则 $B\lhd O_F$ 且 $m!A=(\beta O_F)B$。因此 $A\simeq B$(O_F-模同构，即 A,B 在 $\mathrm{Cl}(O_F)$ 的同一理想类)。但 $\beta\in A$，于是 $m!\beta\in(\beta O_F)B$，因此

由 O_F 为整环知,$m!\in B$。又由引理 7.4 知 $|O_F/m!O_F|<\infty$。因此 $|\{B\lhd O_F \mid m!\in B\}|<\infty$。注意(最小的)$m$ 是由 F 惟一确定的,因此 $\forall\, 0\neq A\lhd O_F$ 必与这有限个之一的 B 是 O_F-模同构的,故 $h_F<\infty$。 □

由此定理立得

推论 23.2 设 F 为数域,O_F 为其代数整元环,$A\lhd O_F$,则必有 $k\mid h_F$,使 A^k 为 O_F 的主理想。

令上述定理证明中由 F 确定的常数 $|O_F/m!O_F|=C$,则又得

命题 23.4 设 F 为数域,O_F 为其代数整元环,则有由 F 确定的常数 C 满足:对 $\mathrm{Cl}(O_F)$ 中任一元素(等价类),都有代表元 $0\neq A\lhd O_F$ 使 $\|A\|<C$。

关于这个界 C,对二次域已有如下的优美结果(见[Hasse, 1980])。

命题 23.5 设 O_F 为 $\mathbb{Q}(\sqrt{d})$($d\in\mathbb{Z}$ 无平方因子)的代数整元环,则对类群 $\mathrm{Cl}(O_F)$ 中的每一个元素(等价类),必有代表元 $0\neq A\lhd O_F$ 使

$$\|A\|\leqslant b=\begin{cases}\sqrt{d}, & d>0\text{ 且 }d\equiv 2,3\pmod 4\\ \sqrt{d}/2, & d>0\text{ 且 }d\equiv 1\pmod 4\\ 2(\sqrt{|d|/3}), & d<0\text{ 且 }d\equiv 2,3\pmod 4\\ \sqrt{|d|/3}, & d<0\text{ 且 }d\equiv 1\pmod 4\end{cases}$$

因此

(1) 在任何情况下,对 $\mathrm{Cl}(O_F)$ 的任一元素,都有代表元 $0\neq A\lhd O_F$ 使得 $\|A\|\leqslant b\leqslant 2(\sqrt{|d|/3})$;

(2) 当素数 $p>b$ 时,$\|pO_F\|>b$(由命题 23.3),因此只要考察 $\leqslant b$ 的素数 p。

这里值得注意的是,属于 $\mathrm{Cl}(O_F)$ 同一等价类的理想,其范未必相同。比如任意主理想 $aO_F\simeq O_F$,但 $\|aO_F\|$ 一般地大于 1,而 $\|O_F\|=1$。

至于对主理想的判定,(判定 A 为 O_F 的主理想,可知 $\langle A\rangle$ 在 $\mathrm{Cl}(O_F)$ 中是单位元)。有下述结果可供使用。

命题 23.6 设 O_F 为 $\mathbb{Q}(\sqrt{d})$($d\in\mathbb{Z}$ 无平方因子)的代数整元环,$0\neq A\lhd O_F$ 且 $\|A\|=n$。

(1) $d\equiv 2,3\pmod 4$ 时,若 A 为 O_F 的主理想(即 $\langle A\rangle$ 平凡),则不定方程 $x^2-dy^2=n$ 或 $x^2-dy^2=-n$ 有整数解;

(2) $d\equiv 1\pmod 4$ 时,若 A 为 O_F 的主理想,则不定方程 $(2x+y)^2-dy^2=4n$ 或 $(2x+y)^2-dy^2=-4n$ 有整数解。

证 记

$$\alpha=\begin{cases}\sqrt{d}, & d\equiv 2,3(\mathrm{mod}\ 4)\\ \frac{1}{2}(1+\sqrt{d}), & d\equiv 1(\mathrm{mod}\ 4)\end{cases}$$

当 $A=aO_F$(即 A 为主理想)时,记 $a=x+\alpha y$,由命题 23.3(4)知 $|N(a)|=\|A\|$。于是在 $d\equiv2,3(\mathrm{mod}\ 4)$时 $\alpha=\sqrt{d}$,$N(a)=x^2-dy^2=n$ 或 $x^2-dy^2=-n$ 必有整数解。

类似地可证 $d\equiv1(\mathrm{mod}\ 4)$的情况。 □

由命题 23.1 又可得有助于类数计算的下述结果。

命题 23.7 设 O_F 为 $F=\mathbb{Q}(\sqrt{d})$($d\in\mathbb{Z}$ 无平方因子)的代数整元环,p 为素数。

(1) 若 p 在 O_F 中是分歧的,则$\langle\hat{p}\rangle\in \mathrm{Cl}(O_F)$的阶数为 1(平凡的)或 2,当 $d\equiv2,3(\mathrm{mod}4)$,$x^2-dy^2=\pm p$ 无整解时,$\mathrm{Ord}\langle\hat{p}\rangle=2$;

(2) 若 p 在 O_F 中是惯性的,则$\langle pO_F\rangle\in \mathrm{Cl}(O_F)$的阶数为 1(平凡的);

(3) 若 p 在 O_F 中是分裂的,则对 p 的素因子 P_1,P_2,$\langle P_1\rangle=\langle P_2\rangle^{-1}$,且 $\|P_1\|=\|P_2\|=p$,同时,$d=2,3(\mathrm{mod}4)$且 $x^2-dy^2=\pm p$ 无整解时,$\mathrm{Ord}\langle P_j\rangle=2$, $j=1,2$。

证 (1) p 在 O_F 中分歧时,$O_F\simeq pO_F=\hat{p}^2$. 因此$\langle\hat{p}\rangle$的阶数为 1 或 2。又显然 $d\equiv2,3(\mathrm{mod}4)$,$x^2-dy^2=\pm p$ 无整解时,$\hat{p}$非主理想,$\mathrm{ord}\langle\hat{p}\rangle=2$。

(2) p 在 O_F 中是惯性的时,由于 pO_F 为主理想,因此$\langle pO_F\rangle=\langle O_F\rangle$,其阶数为 1。

(3) p 在 O_F 中分裂时,$O_F\simeq pO_F=P_1P_2$。因此$\langle P_1\rangle=\langle P_2\rangle^{-1}$且

$$O_F/pO_F\simeq O_F/P_1P_2\simeq O_F/P_1\oplus O_F/P_2,\ O_F/P_j\simeq\mathbb{Z}_p,\ j=1,2$$

故 $\|P_1\|=\|P_2\|=p$。又 $d\equiv2,3(\mathrm{mod}4)$,$x^2-dy^2=\pm p$ 无整解时,P_j 非主理想,$\mathrm{Ord}\langle P_j\rangle=2$,$j=1,2$。 □

现在,我们用上述结果计算几个例子($p>3$,$p\equiv3(\mathrm{mod}\ 4)$时关于$\mathbb{Q}(\sqrt{-p})$的类数计算法已由上节末给出,这里以其他情况作例)。

例 1 $F=\mathbb{Q}(\sqrt{-3})$,$-3\equiv1(\mathrm{mod}\ 4)$,$O_F=\mathbb{Z}[\frac{1}{2}(1+\sqrt{-3})]$。

由命题 23.5 知 $\mathrm{Cl}(O_F)$的一切等价类都有 A 使 $\|A\|\leqslant\sqrt{\frac{3}{3}}=1$,因此 $\|A\|=1$,亦即$|O_F/A|=1$。于是 $\mathrm{Cl}(O_F)=1$,即 $h_F=1$,由此知

$$K_0(\mathbb{Z}[\frac{1}{2}(1+\sqrt{-3})])\simeq\mathbb{Z}$$

且

$$\mathbb{Z}[\frac{1}{2}(1+\sqrt{-3})]\in \text{UFD}$$

用此法同样可证，$K_0(\mathbb{Z}[\frac{1}{2}(1+\sqrt{-11})])\simeq\mathbb{Z}$，$K_0(\mathbb{Z}[\frac{1}{2}(1+\sqrt{-19})])\simeq\mathbb{Z}$。因此 $\mathbb{Z}[\frac{1}{2}(1+\sqrt{-d})]$ 当 $d=11,19$ 时，也为 UFD。

例 2　$F=\mathbb{Q}(\sqrt{-21})$，$-21\equiv 3(\mathrm{mod}\ 4)$，$O_F=\mathbb{Z}[\sqrt{-21}]$。

由命题 23.5 知只需考察 $\|A\|\leqslant 2(\sqrt{21/3})=2\cdot\sqrt{7}<6$。于是只需考察素数 2,3,5($p>5$ 由此命题知无需考虑)。由命题 23.2 容易看出：

2 是分歧的，$\hat{2}=(2,1+\sqrt{-21})$；由于 $3\mid 21$，3 也是分歧的，$\hat{3}=(3,\sqrt{-21})$；又由于 $-21=2^2(\mathrm{mod}\ 5)$，5 为分裂的，$5_1=(5,2+\sqrt{-21})$，$5_2=(5,2-\sqrt{-21})=5_1^{-1}$。因此

$$\mathrm{Cl}(\mathbb{Z}[\sqrt{-21}])=\langle\{\langle\hat{2}\rangle,\langle\hat{3}\rangle,\langle 5_1\rangle,\langle 5_2\rangle\}\rangle$$

而 $\|\hat{2}\|=2$，$\|\hat{3}\|=3$，$\|\hat{2}\cdot\hat{3}\|=6$，$x^2+21y^2=\pm 2,\pm 3,\pm 6$ 都无整数解。因此 $\langle\hat{2}\rangle,\langle\hat{3}\rangle,\langle\hat{2}\cdot\hat{3}\rangle$ 都非平凡(不为单位元)，又由命题 23.7 知 $\langle\hat{2}\rangle,\langle\hat{3}\rangle$ 的阶数都是 2。由此知 $\langle\hat{2}\cdot\hat{3}\rangle=\langle\hat{2}\rangle\cdot\langle\hat{3}\rangle\neq\langle\hat{2}\rangle,\langle\hat{3}\rangle$。又 $x^2+21y^2=\pm 5$ 亦无整数解，于是 $\langle 5_1\rangle,\langle 5_2\rangle$ 非平凡，从而都是 2 阶元(因为 $5_2=5_1^{-1}$ 即 $5_2^2=1=\langle O_F\rangle$)。因此由上知 $\langle\hat{2}\rangle\langle\hat{3}\rangle=\langle 5_j\rangle$，$j=1$ 或 2，令 $a=\langle\hat{2}\rangle$，$b=\langle\hat{3}\rangle$，则

$$\mathrm{Cl}(\mathbb{Z}[\sqrt{-21}])\simeq\{a,b\mid a^2=b^2=1,ab=ba\}\simeq\mathbb{Z}_2\oplus\mathbb{Z}_2$$

为 Klein 四元群。于是 $h_F=4$，

$$K_0(\mathbb{Z}[\sqrt{-21}])\simeq\mathbb{Z}\oplus\mathbb{Z}_2\oplus\mathbb{Z}_2$$

注①　设 K 为有限域，$Q=K(X)$(与代数数域合称为**整体域**(global field))，则对任意既约多项式 $p[X]\in K[X]$，$K[X]/p(X)K[X]$ 都是有限域. $K[X]$ 的剩余类环也都是有限环。于是 $\forall\,0\neq A\lhd K[X]$，$\|A\|<\infty$，也可证 Q 的有限次扩张的代数整元环的类数必是有限的。

最后，我们举一个特征数 $\neq 2$ 的有理函数域的例子并给出两个注以结束本节。

例 3　设 K 为域，$\mathrm{Ch}K\neq 2$，$Q=K(X)$，$d=d(X)\in K[X]$ 无平方因子。

(1) $\deg d(X)=1$ 时，经变元的改换，可令 $d(X)=X$，$F=Q(\sqrt{X})=K(Y)$，其中 $Y^2=X$，其代数整元环 $O_F=K[X][\sqrt{X}]=K[Y]\in\text{PID}$。因此，$h_F=1$，$O_F$ 为抛物线(parabola)$Y^2=X$ 的坐标环。

(2) $\deg d(X)=2$ 时，经变元的改换可取 $d=d(X)=aX^2+b$。此时 $O_F=K[X][\sqrt{d}]$为二次曲线 $Y^2=aX^2+b$ 的坐标环。

(i) Y^2-aX^2 既约(作为两个变元的多项式)，则对应的二次曲线为"椭圆"(ellipse)，可算出$\mathrm{Cl}(O_F)\simeq\mathbb{Z}_2$，即 $h_F=2$。比如取 $K=\mathbb{F}$，$d(X)=1-X^2$，则

$$O_F=\mathbb{F}[X,Y]/(X^2+Y^2-1)$$

为单位圆的坐标环。

(ii) Y^2-aX^2 可约时，则对应的二次曲线为双曲线(hyperbola)，可算出 $\mathrm{Cl}(O_F)=1$。比如取 $K=\mathbb{F}$，$d(X)=X^2+1$，则

$$O_F=\mathbb{F}[X,Y]/(Y^2-X^2-1)$$

为双曲线的坐标环。

(3) $\deg d(X)=3$ 时，曲线 $Y^2=d(X)$ 为**椭圆曲线**(elliptic curve)即亏格(genus)为 1 的曲线，其标准方程为 $y^2=x^3+k$。这方面研究已较深刻，结果十分丰富。在代数几何与数论中都有重要应用。

注② 1966 年 L. J. Mordell 证明了：若 $y^2=x^3+k$，k 无 6 次幂因子且 $y^2=x^3+k$ 有一组有理解(x,y)，$xy\neq 0$，则当 $k\neq 1,-432$ 时，必有无穷多组有理解，即椭圆曲线 $y^2=x^3+k$ 上有一个(两坐标均非零的)非零有理点则必有无穷多个有理点(在上述 k 的限制条件下)。

此外，可以证明：(1) 设 $d>1$ 无平方因子且 $d\equiv 1,2 \pmod 4$，同时 $\mathbb{Q}(\sqrt{-d})$的(代数整元环的)类数不是 3 的倍数，则椭圆曲线 $y^2=x^3-d$ 上有整点$\Leftrightarrow d=3t^2\pm 1$，$t\in\mathbb{Z}$. 此时这些整点为$(t^2+d,\pm t(t^2-3d))$。

由此结果可知：$y^2=x^3-2$ 的整解全体为 $x=3$，$y=\pm 5$(此时 $h=1$，$d=2$)；$y^2=x^3-13$ 的整解全体为 $x=17$，$y=\pm 70$(此时 $h=1$，$d=13$)。

(2) 设 $d>0$，$d\neq 7$ 无平方因子且$\mathbb{Q}(\sqrt{-d})$的类数 $h=3$，$d=a^2+b^3$，$b\equiv 2,3 \pmod 4$，a 无 $4t+3$ 形的素因子，则 $y^2=x^3-d$ 无整解(见[柯召，1980])。

由此知 $y^2=x^3-31$ 无整数解(此时 $h=3$，$31=2^2+3^3$)。

由上述两结果可看出：类数的计算与不定方程的解也有着有趣的关系。

注③ 类数也与多项式表示素数的问题有关，比如 1974 年 M. D. Hendy 证出：若二素数 $p<q$，$pq\equiv 3 \pmod 4$，$f(x)=px^2+px+(p+q)/4$，则 $k=0,1,\cdots,\frac{p+q}{4}-2$ 时 $f(k)$均为素数$\Leftrightarrow\mathbb{Q}(\sqrt{-p})$的类数 $h=2$. (A. Baker(1969, 1971)，H. L. Montgomery 与 P. J. Weinberger(1974)，以及 H. M. Stark(1975)已定出使$\mathbb{Q}(\sqrt{-d})$之类数为 2 的全体 d 的值：5，6，10，13，15，22，35，37，51，

58,91,115,123,187,235,267,403,427（类数为 1 的全体 d 值见上节）。

值得注意的是：不能期望找到一个整系数一元多项式，使它在任意整数的值全为素数。事实上可证：设 $f(x)\in\mathbb{Z}[x]\setminus\mathbb{Z}$，则有无限多个 n，使 $|f(n)|$ 不是素数。（可令 $n_0\geqslant 0$ 使 $|f(n_0)|=p$ 为素数（否则结论已真），由 $\lim\limits_{x\to\infty}|f(x)|=\infty$ 知必有 $n_1>n_0$ 使当 $n\geqslant n_1$ 时 $|f(n)|>p$。因此 $n_0+ph\geqslant n_1$，$h\in\mathbb{N}$ 时，$f(n_0+ph)=f(n_0)+p$ 的倍数，而 $|f(n_0+ph)|>p$，于是 $|f(n_0+ph)|$ 为合数）。尽管如此，多项式表素数的问题仍一直是一个有兴趣的问题。比如，对多项式 x^2+x+p（p 为素数），下述三点等价：(1) $p=2,35,11,17,41$；(2) x^2+x+p 当 $x=0,1,\cdots,p-2$ 时取素数值；(3) $\mathbb{Q}(\sqrt{1-4p})$ 的类数为 1。(1)⇒(2)在 1772 年即由 J. A. Euler 给出。F. G. Frobenius 在 1912 年证出(3)⇒(2)，而(1)⇒(3)在 Gauss 生前即已知道。1912 年 G. Rabinovitch 给出(2)⇔(3)。1987 年由 P. Ribenbioim 给出三者等价的初等证明（见[Ribenboim，1989]）。

与此相关的有两个具体例子：x^2-x+17，$x=1,\cdots 16$ 时均给出素数；x^2-x+41 当 $x=1,2,\cdots,40$ 时都给出素数，自然要问：任给正整数 $N>1$，是否有素数 p 使 x^2-x+p，当 $x=1,2,\cdots,N$ 时都给出素数？事实上这是一个比孪生素数问题（差为 2 的素数对是否有无穷多对?）更难的悬题。因为若本问题有肯定的解答，取 $p_1\geqslant 3$ 为素数，则有素数 p_2 使 $x=1,2,\cdots,p_1$ 时 x^2-x+p_2 为素数。当然 $p_2>p_1$（$x=p_2$ 时上式不能给出素数），以此类推，则有素数列 $p_1<p_2<p_3<\cdots$，使 $x=1,2,\cdots,p_{i-1}$ 时，x^2-x+p_i 为素数。取 $x=1,2$，即得无穷多对孪生素数(p_i,p_i+2)，$i=2,3,\cdots$，从而即“解决”了孪生素数问题。取 $x=1,2,3$ 又得无穷多组三生素数(p_i,p_i+2,p_i+6)，$i=2,3,\cdots$ 从而“解决”了所谓的“三生素数”难题，由此也可看出，多项式表达素数的研究是有意义的工作。

§24　Descartes 方图导出的行正合交换图及其应用

设 $\mathcal{C}$Ring 中有 Descartes 方图

$$\begin{array}{ccc} R & \xrightarrow{i_2} & R_2 \\ {\scriptstyle i_1}\downarrow & & \downarrow{\scriptstyle j_2} \\ R_1 & \xrightarrow[j_1]{} & S \end{array} \tag{1}$$

其中 j_2(或 j_1)为满同态. 按 § 17 记号,记 $P=(P_1,P_2,h)$, $P'=(P_1',P_2',h')$,则有 S-模同构

$$h\otimes h':(S\underset{j_1}{\otimes}P_1)\underset{S}{\otimes}(S\underset{j_1}{\otimes}P')\to(S\underset{j_2}{\otimes}P_2)\underset{S}{\otimes}(S\underset{j_2}{\otimes}P_2')$$

$$\wr|\qquad\qquad\qquad\wr|$$

$$S\underset{j_1}{\otimes}(P_1\underset{R_1}{\otimes}P_1')\qquad S\underset{j_2}{\otimes}(P_2\underset{R_2}{\otimes}P_2')$$

且 $h\otimes h'(1\otimes(x_1\otimes x_1'))=1\otimes(x_2\otimes x_2')$, $\forall x_j\in P_j, x_j'\in P_j', j=1,2$. 我们记

$$Q=(P_1\underset{R_1}{\otimes}P_1',\ P_2\underset{R_2}{\otimes}P_2',\ h\otimes h')$$

来证 $Q\simeq P\underset{R}{\otimes}P'\in {}_R\mathfrak{M}$。即

命题 24.1 设(1)为⊃Ring 中的 Descartes 方图,其中 j_2 或 j_1 为满同态,$P\simeq(P_1,P_2,h)$, $P'\simeq(P_1',P_2',h')\in$ f. g. $\mathrm{P}_R\mathfrak{M}$, $Q=(P_1\underset{R_1}{\otimes}P_1',P_2\underset{R_2}{\otimes}P_2',h\otimes h')$,则有 R-模同构

$$Q\simeq P\underset{R}{\otimes}P'$$

证 由 § 17 知,$P\underset{R}{\otimes}P'$可写成

$$P\underset{R}{\otimes}P'=(R_1\underset{i_1}{\otimes}(P\underset{R}{\otimes}P'),R_2\underset{i_2}{\otimes}(P\underset{R}{\otimes}P'),\ h_{P\otimes P'}),$$

其中

$$h_{P\otimes P'}:S\underset{j_1}{\otimes}(R_1\underset{i_1}{\otimes}(P\underset{R}{\otimes}P'))\to S\underset{j_2}{\otimes}(R_2\underset{i_2}{\otimes}(P\underset{R}{\otimes}P'))$$

为 S-模同构。

注意显然有 R_j-模同构

$$u_j:R_j\underset{i_j}{\otimes}(P\underset{R}{\otimes}P')\to P_j\underset{R_j}{\otimes}P_j',\qquad j=1,2.$$

直接验证下图是交换图即得本命题

$$\begin{array}{ccc}
S\underset{j_1}{\otimes}R_1\underset{i_1}{\otimes}(P\underset{R}{\otimes}P') & \xrightarrow[\simeq]{h_{P\otimes P'}} & S\underset{j_2}{\otimes}R_2\underset{i_2}{\otimes}(P\underset{R}{\otimes}P') \\
1\otimes u_1\downarrow\simeq & & \simeq\downarrow 1\otimes u_2 \\
S\underset{j_1}{\otimes}(P_1\underset{R_1}{\otimes}P_1') & \xrightarrow[h\otimes h']{\simeq} & S\underset{j_2}{\otimes}(P_2\underset{R_2}{\otimes}P_2')
\end{array}$$

□

为研究 Picard 群,由上命题先来证如下命题。

命题 24.2 设(1)为⊃Ring 中的 Descartes 方图,其中 j_2 或 j_1 为满同态,$P=(P_1,P_2,h)\in$ f. g. $\mathrm{P}_R\mathfrak{M}$,则 P 为可逆 R-模⇔P_j 为可逆 R_j-模,$j=1$,2。

证 ⇒:设 P 为可逆 R-模,则有 $P'=(P_1',P_2',h')\in {}_R\mathfrak{M}$ 使 $P\underset{R}{\otimes}P'\simeq R$。由命题 24.1 知

$$(P_1 \underset{R_1}{\otimes} P_1', P_2 \underset{R_2}{\otimes} P_2', h \otimes h') \simeq P \underset{R}{\otimes} P' \simeq R \overset{\S 17}{\simeq} (R_1, R_2, I),$$

于是

$$P_j \underset{R_j}{\otimes} P_j' \simeq R_j, \qquad j = 1,2$$

因此 P_j 为可逆 R_j-模，$j=1,2$。

$\Leftarrow$：设 P_j 为可逆 R_j-模，$j=1,2$。记 $P_j^* = \mathrm{Hom}_{R_j}(P_j, R_j)$，则有 R_j-模同构

$$\lambda_j : P_j \underset{R_j}{\otimes} P_j^* \xrightarrow{\simeq} R_j, \qquad j = 1,2$$

但由 S-模同构

$$h: S \underset{j_1}{\otimes} P_1 \to S \underset{j_2}{\otimes} P_2$$

知，必有 S-模同构

$$k: S \underset{j_1}{\otimes} P_1^* \to S \underset{j_2}{\otimes} P_2^*$$

即 $P^* = (P_1^*, P_2^*, k) \in \mathrm{f.g.P}_R\mathfrak{M}$，于是命题 24.1 知，有 R-模同构

$$P \underset{R}{\otimes} P^* \simeq (P_1 \underset{R_1}{\otimes} P_1^*, P_2 \underset{R_2}{\otimes} P_2^*, h \otimes k)$$

再由交换图

$$\begin{array}{ccc}
S \underset{j_1}{\otimes} (P_1 \underset{R_1}{\otimes} P_1^*) & \xrightarrow[\simeq]{h \otimes k} & S \underset{j_2}{\otimes} (P_2 \underset{R_2}{\otimes} P_2^*) \\
1 \otimes \lambda_1 \downarrow \simeq & & \simeq \downarrow 1 \otimes \lambda_2 \\
S \simeq S \underset{j_1}{\otimes} R_1 & \xrightarrow[I]{\simeq} & S \underset{j_2}{\otimes} R_2 \simeq S
\end{array}$$

即知有 R-模同构 $P \underset{R}{\otimes} P^* \simeq (R_1, R_2, I) \simeq R$。故 P 为可逆 R-模。 □

参照§17，对上述 Descartes 方图可定义 $f_1, g_1, \delta, f_0, g_0$ 使

$$R^{\cdot} \xrightarrow{f_1} R_1^{\cdot} \oplus R_2^{\cdot} \xrightarrow{g_1} S^{\cdot} \xrightarrow{\delta} \mathrm{Pic}(R) \xrightarrow{f_0}$$

$$\mathrm{Pic}(R_1) \oplus \mathrm{Pic}(R_2) \xrightarrow{g_0} \mathrm{Pic}(S) \tag{2}$$

构成群的同态列。其中

$f_1 = (i_1 \oplus i_2)\Delta$，即 $\forall \alpha \in R^{\cdot}$，$f_1(\alpha) = (i_1(\alpha), i_2(\alpha))$；

$g_1 = \Delta^-(j_1 \oplus j_2)$，即 $\forall \beta_j \in R_j^{\cdot}$，$g_1(\beta_1, \beta_2) = j_1(\beta_1)(j_2(\beta))^{-1}$；

注意 $\forall \gamma \in S^{\cdot} = \mathrm{GL}_1(S)$，由命题 24.2，$(R_1, R_2, \gamma)$ 为可逆 R-模。定义

$\delta(\gamma) = \langle R_1, R_2, \gamma \rangle \equiv \langle (R_1, R_2, \gamma) \rangle$，$\forall \gamma \in S^{\cdot}$；

$f_0(\langle P_1, P_2, h \rangle) = (\langle P_1 \rangle \langle P_2 \rangle)$，$\forall \langle P_1, P_2, h \rangle \in \mathrm{Pic}(R)$；

$g_0((\langle P_1 \rangle, \langle P_2 \rangle)) = \langle S \underset{j_1}{\otimes} P_1 \rangle \langle S \underset{j_2}{\otimes} P_2 \rangle^{-1}$，$\forall \langle P_j \rangle \in \mathrm{Pic}(R_j)$，$j=1,2$。

下面来证(2)为群正合列且有下面的交换图(3),即

命题 24.3 设(1)为$\mathcal{C}$Ring 中的 Descartes 方图,其中 j_2 或 j_1 为满同态。则有(Abel)群行正合的交换图

$$\begin{array}{ccccccccccc}
K_1(R) & \xrightarrow{f_1} & K_1(R_1)\oplus K_1(R_2) & \xrightarrow{g_1} & K_1(S) & \xrightarrow{\delta} & K_0(R) & \xrightarrow{f_0} & K_0(R_1)\oplus K_0(R_2) & \xrightarrow{g_0} & K_0(S)\\
\det\downarrow & & \det\oplus\det\downarrow & & \det\downarrow & & \det\downarrow & & \det\oplus\det\downarrow & & \det\downarrow\\
R^{\cdot} & \xrightarrow[f_1]{} & R_1^{\cdot}\oplus R_2^{\cdot} & \xrightarrow[g_1]{} & S^{\cdot} & \xrightarrow[\delta]{} & \mathrm{Pic}(R) & \xrightarrow[f_0]{} & \mathrm{Pic}(R_1)\oplus\mathrm{Pic}(R_2) & \xrightarrow[g_0]{} & \mathrm{Pic}(S)
\end{array} \qquad (3)$$

其中上行的 f_1,g_1,δ,f_0,g_0 的定义见 § 17。左边三个竖直箭头所示的同态 det 为交换环上矩阵行列式诱导的同态($\overline{A}\mapsto \det A$)。右边三个竖直箭头所示的同态 det 的定义见 § 21 命题 21.1($\det=\tau\pi:[M]\mapsto\langle\Lambda^n N\rangle$),为简化记号,与左边的三个不另加区别。

证 为简化记号,而又与上行的同态相区别,在以下证明中将(3)中下行的同态 f_1,g_1,δ,f_0,g_0 分别记为$\underline{f_1},\underline{g_1},\underline{\delta},\underline{f_0},\underline{g_0}$。

由 § 18 已知(3)的上行正合。又(3)的交换性可直接验证(只需注意:$\det:K_0(R)\to\mathrm{Pic}(R)$ 使 $\det([P_1,P_2,h])=\langle\det P_1,\det P_2,\det h\rangle$)。

现证(3)中的下行是正合的即可。事实上,由(3)是交换图以及上行正合可知下行为复形,这是因为

$$g_1f_1=0(\text{上行正合})\Rightarrow\det\cdot g_1f_1=0\underset{(3)\text{交换}}{\Rightarrow}\underline{g_1}\,\underline{f_1}\cdot\det=0$$

$$\underset{\det\text{满}}{\Rightarrow}\underline{g_1}\,\underline{f_1}=0$$

同理知$\underline{\delta}\underline{f_1}=0,\underline{f_0}\underline{\delta}=0,\underline{g_0}\,\underline{f_0}=0$。由此知,只需再证:$\mathrm{Ker}\,\underline{g_1}\subseteq\mathrm{Im}\,\underline{f_1}$,$\mathrm{Ker}\underline{\delta}\subseteq\mathrm{Im}\,\underline{g_1}$,$\mathrm{Ker}\,\underline{f_0}\subseteq\mathrm{Im}\,\underline{\delta}$,$\mathrm{Ker}\,\underline{g_0}\subseteq\mathrm{Im}\,\underline{f_0}$。

(1) $\forall(\alpha_1,\alpha_2)\in\mathrm{Ker}\,\underline{g_1}$,必 $j_1(\alpha_1)=j_2(\alpha_2)$,因此由 Descartes 图的定义,必有惟一的 $\alpha\in R$ 使 $i_l(\alpha)=\alpha_l,l=1,2$。下证 $\alpha\in R^{\cdot}$ 即知

$$(\alpha_1,\alpha_2)=(i_1(\alpha),i_0(\alpha))=\underline{f_1}(\alpha)\in\mathrm{Im}\,\underline{f_1}$$

事实上,由 $j_1(\alpha_1)=j_2(\alpha_2)$知,$j_1(\alpha_1^{-1})=j_2(\alpha_2^{-1})$,于是有惟一的 $\alpha'\in R$ 使 $i_l(\alpha')=\alpha_l^{-1},l=1,2$。但 $j_1(1)=j_2(1)=1$。于是有惟一的 $\alpha''\in R$ 使 $i_l(\alpha'')=1$(这里的 1 各表示相应环的单位元),$l=1,2$。由此知 $\alpha''=1$。而

$$i_l(\alpha\alpha')=i_l(\alpha)i_l(\alpha')=\alpha_l\alpha_l^{-1}=1$$

因此又知 $\alpha\alpha'=1$,即 $\alpha\in R^{\cdot}$ 。

(2) $\forall\alpha\in\mathrm{Ker}\,\underline{\delta}$。在 $\mathrm{Pic}(R)$ 中必有$\langle R_1,R_2,\alpha\rangle=\langle R\rangle=\langle R_1,R_2,I\rangle$,因此有 R-模同构:$(R_1,R_2,\alpha)\simeq(R_1,R_2,I)$。由 § 17 知此同构可表为$(\alpha_1,\alpha_2)$:$(R_1,R_2,\alpha)\to(R_1,R_2,I)$,其中 $\alpha_1:R_1\to R_1$ 为 R_1-模同构. 因此 $\alpha_1\in GL_1(R)=R_1^{\cdot}$(同理 $\alpha_2\in R_2^{\cdot}$),且有交换图

$$\begin{array}{ccc} S\simeq S\underset{j_1}{\otimes}R_1 & \xrightarrow[\simeq]{\alpha} & S\underset{j_2}{\otimes}R_2\simeq S \\ 1\otimes\alpha_1\downarrow\simeq & & \simeq\downarrow 1\otimes\alpha_2 \\ S\simeq S\underset{j_1}{\otimes}R_1 & \xrightarrow[I]{\simeq} & S\underset{j_2}{\otimes}R_2\simeq S \end{array}$$

由此知有交换图

$$\begin{array}{ccc} S & \xrightarrow[\simeq]{\alpha} & S \\ j_1\alpha_1\downarrow\simeq & & \simeq\downarrow j_2\alpha_2 \\ S & \xrightarrow[I]{\simeq} & S \end{array}$$

于是 $\alpha=(j_1\alpha_1)(j_2\alpha_2)^{-1}=\underline{g_1}(\alpha_1,\alpha_2)\in\operatorname{Im}\underline{g_1}$。

(3) $\forall\langle P_1,P_2,h\rangle\in\operatorname{Ker}f_0$，必有 $\langle P_j\rangle=1\in\operatorname{Pic}(R_j)$，$j=1,2$。因此有 R_j-模同构 $\alpha_j:P_j\to R_j$，$j=1,2$。于是可定义 S-模同构 $k:S\to S$ 使下图为交换图。

$$\begin{array}{ccc} S\underset{j_1}{\otimes}P_1 & \xrightarrow[\simeq]{h} & S\underset{j_1}{\otimes}P_2 \\ 1\otimes\alpha_1\downarrow\simeq & & \simeq\downarrow 1\otimes\alpha_2 \\ S\underset{j_1}{\otimes}R_1 & \xrightarrow[k]{\simeq} & S\underset{j_2}{\otimes}R_2 \end{array}$$

由此知 $(\alpha_1,\alpha_2):(P_1,P_2,h)\to(R_1,R_2,k)$ 为 R-模同构。故 $\langle P_1,P_2,h\rangle=\langle R_1,R_2,k\rangle$. 再由 $k\in GL_1(S)=S^{\cdot}$ 即知

$$\langle R_1,R_2,k\rangle=\underline{\delta}(K)\in\operatorname{Im}\underline{\delta}$$

即 $\langle P_1,P_2,h\rangle\in\operatorname{Im}\underline{\delta}$。

(4) $\forall(\langle P_1\rangle,\langle P_2\rangle)\in\operatorname{Ker}\underline{g_0}$，必有 $\langle S\underset{j_1}{\otimes}P_1\rangle=\langle S\underset{j_2}{\otimes}P_2\rangle$。于是有 S-模同构 $h:S\underset{j_1}{\otimes}P_1\to S\underset{j_2}{\otimes}P_2$。因此由命题 24.2 知 $\langle P_1,P_2,h\rangle\in\operatorname{Pic}(R)$ 使

$$(\langle P_1\rangle,\langle P_2\rangle)=\underline{f_0}(\langle P_1,P_2,h\rangle)\in\operatorname{Im}\underline{f_0}\qquad\square$$

命题 24.4　设(1)为 CRing 中的 Descartes 方图，其中 $j_1|_{R_1^{\cdot}}$（或 $j_2|_{R_2^{\cdot}}$）是满映射，则

(1) 图(3)的下行中 g_1 为满同态，f_0 为单同态，且

$$\operatorname{Im}g_0\simeq(\operatorname{Pic}(R_1)\oplus\operatorname{Pic}(R_2))/\operatorname{Pic}(R)\underset{\simeq}{<}\operatorname{Pic}(S);$$

(2) 当 $\operatorname{Pic}(S)=1$ 时，$\operatorname{Pic}(R)\simeq\operatorname{Pic}(R_1)\oplus\operatorname{Pic}(R_2)$。

证　由 j_2 为环同态知必有 $r_2\in R_2$，使 $j_2(r_2)=1$（S 的单位元）且由 $j_1|_{R_1^{\cdot}}$ 满知 $\forall u\in S^{\cdot}$ 必有 $r_1\in R_1^{\cdot}$ 使 $j_1(r_1)=u$。因此 $g_1(r_1,r_2)=u$。由此知 g_1 是满的，于是由(3)之下行正合知 $\delta=0$，且 f_0 为单的。于是

$$\mathrm{Ker}g_0 = \mathrm{Im}f_0 \simeq \mathrm{Pic}(R)$$

由此即知

$$\mathrm{Im}g_0 \simeq (\mathrm{Pic}(R_1) \oplus \mathrm{Pic}(R_2))/\mathrm{Ker}g_0$$
$$\simeq (\mathrm{Pic}(R_1) \oplus \mathrm{Pic}(R_2))/\mathrm{Pic}(R) \underset{\simeq}{\leq} \mathrm{Pic}(S)$$

由(1)得(2)是显然的。 □

作为此命题的应用,仍以 § 18 中的群环 $\mathbb{Z}G=\mathbb{Z}\mathbb{Z}_p$ 作例,来证

推论 24.1 设 $G=\{1,g,\cdots,g^{p-1}\}\simeq\mathbb{Z}_p$ 为 p 阶循环群,p 为素数,$\xi=e^{\frac{2\pi}{p}}$ 为 p 次分圆本原单位根。则

$$\mathrm{Pic}(\mathbb{Z}G) \simeq \mathrm{Pic}\mathbb{Z}[\xi] \simeq \mathrm{Cl}(\mathbb{Z}[\xi])(\simeq \widetilde{\mathrm{K}}_0(\mathbb{Z}[\xi]) \simeq r\mathrm{K}_0(\mathbb{Z}[\xi]))$$

证 由 § 18,有 Descartes 方图(其中 $j_1(\xi)=\overline{1}$)。

$$\begin{array}{ccc} \mathbb{Z}G & \xrightarrow{i_2} & \mathbb{Z} \\ i_1\downarrow & & \downarrow j_2 \\ \mathbb{Z}[\xi] & \xrightarrow{j_1} & \mathbb{Z}_p \end{array}$$

由 $1+\xi+\cdots^{p-1}=0$ 知 $r_1=1+\xi+\cdots+\xi^{p-2}=-\xi^{p-1}$,$(-\xi)(-\xi^{p-1})=1$ 于是 $r_1\in\mathbb{Z}[\xi]^{\cdot}$,$j_1(r_1)=p-1$。由此知 $j_1|_{\mathbb{Z}[\xi]^{\cdot}}:\mathbb{Z}[\xi]^{\cdot}\to\mathbb{Z}_p^{\cdot}$ 为满射(注意 $\mathbb{Z}_p^{\cdot}$ 为循环群阶数为 $p-1$)。但 $\mathbb{Z}_p$ 为域,$\mathrm{Pic}(\mathbb{Z}_p)=1$,因此由命题 24.4(2)即得证(注意 $\mathbb{Z}[\xi]$ 为 Dedekind 环,结论中右面三个同构由定理 22.1 可知)。 □

注① 可以证明:设 $R\in\mathfrak{C}\mathrm{Ring}$,$G$ 为群,则 RG 为整环 $\Leftrightarrow R$ 为整环且 G 为无挠群(比如见[Karpilovsky,1983])。因此上述的 $\mathbb{Z}G$ 不是整环(但为连通环,见 § 18),从而上述推论给出用 Dedekind 环的 Picard 群(理想类群)计算非整环的 Picard 群的一个佳例,从中又一次看出 Dedekind 环的重要性。

显然,应用(3)计算 Picard 群及 K_0 群等的关键在于构作适当的 Descartes 方图(1)。下面给出较一般的实例。

引理 24.1 在 $\mathfrak{R}\mathrm{ing}$ 中设 $i_2:R\to R_2$ 为单同态(包含映射),$I\lhd R_2$ 且 $I\subseteq R$。$R_1=R/I$,$S=R_2/I$,$i_1:R\twoheadrightarrow R_1$,$j_2:R_2\twoheadrightarrow S$ 为标准同态. $j_1:R_1\to S$ 为 i_2 诱导的标准单同态,则

$$\begin{array}{ccc} R & \xrightarrow{i_2} & R_2 \\ i_1\downarrow & & \downarrow j_2 \\ R_1 & \xrightarrow{j_1} & S \end{array} \tag{4}$$

为(使 j_2 为满同态的)Descartes 方图。

证　图(4)的交换性是显见的。又 $\forall r_2\in R_2, r_1+I=\bar{r}_1\in R_1=R/I$,若 $j_1(r_1+I)=j_2(r_2)$,则 $R_2/I=S$ 中 $r_1+I=r_2+I$。于是由 $I\subseteq R, r_1\in R$ 知 $r_2\in r_1+I\subseteq R$。从而 $i_2(r_2)=r_2, i_1(r_2)=r_2+I=r_1+I, r_2$ 的惟一性是显见的,故(4)为 Descartes 方图。 □

推论 24.2　设 $R_2=\mathbb{Z}[\alpha], \alpha^2=a\alpha+b, a,b\in\mathbb{Z}, x^2-ax-b$ 在 $\mathbb{Z}[x]$ 中不可约。$R=\mathbb{Z}[r\alpha], r>0, r\in\mathbb{Z}, I=rR_2, R_1=R/I, S=R_2/I$,则 $R_1\simeq\mathbb{Z}_r, S\simeq\mathbb{Z}_r[\alpha]=R_1[\alpha]$ 且有 Descartes 方图

$$\begin{array}{ccc}\mathbb{Z}[r\alpha] & \xrightarrow{i_2} & \mathbb{Z}[\alpha]\\ {\scriptstyle i_1}\downarrow & & \downarrow{\scriptstyle j_2}\\ \mathbb{Z}_r & \xrightarrow[j_1]{} & \mathbb{Z}[\alpha]\end{array} \tag{5}$$

其中 $i_1(n+mr\alpha)=\bar{n}(\mathrm{mod}\ r)$,因此为环的满同态,$j_2$ 为标准的环的满同态。

证　显然 $R\subseteq R_2=\mathbb{Z}[\alpha]$。因此有环的单同态,$i_2: R\to R_2$,又由 $I\lhd R_2, I\subseteq R$ 知 $R_1=R/I\simeq\mathbb{Z}_r, S=R_2/I\simeq\mathbb{Z}_r[\alpha]=R_1[\alpha]$,于是由引理 24.1 知(5)为 Descartes 方图。i_1, j_2 为满同态是显见的。 □

推论 24.3　在推论 24.2 中取 $\alpha=\frac{1}{2}(1+\sqrt{-d}), d\in\mathbb{Z}$ 无平方因子,$d>0$ 且 $d\equiv 3(\mathrm{mod}\ 4), r=2$,则 $R=\mathbb{Z}[r\alpha]=\mathbb{Z}[\sqrt{-d}], R_1\simeq\mathbb{Z}_2$(域),$R_2=\mathbb{Z}[\frac{1}{2}(1+\sqrt{-d})], S=\mathbb{Z}_2[\alpha]=R_1[\alpha]$ 且有下述结果(由于 $\mathrm{Pic}(T)\in{}_{\mathbb{Z}}\mathfrak{M}, \forall T\in\mathcal{C}\mathrm{Ring}$。为方便起见,在图中常将 $\mathrm{Pic}(T)=1$(平凡群)记为 $\mathrm{Pic}(T)=0$,且将 $K_1(T)=1$ 记为 $K_1(T)=0$):

d	3,7,…	11,19,23,31,…	15,…
$K_0(R)$	$\mathbb{Z}$	$\mathbb{Z}\oplus\mathbb{Z}_3$	$\mathbb{Z}\oplus\mathbb{Z}_2$
$\mathrm{Pic}(R)\simeq\mathrm{Cl}(R)$	1	$\mathbb{Z}_3$	$\mathbb{Z}_2$
h_p	1	3	2

证　为证本推论,只需分情况地确定 $K_0(R)$ 或 $\mathrm{Pic}(R)$,其他都是显见的。

注意 $d\equiv 3(\mathrm{mod}\ 4)$ 即 $d\equiv 3,7(\mathrm{mod}\ 8)$,此时 $\alpha^2=\alpha-\frac{1}{4}(1+d)$。又由引理 23.2 知,$R_2=\mathbb{Z}[\alpha]$ 为 Dedekind 环(但 $R=\mathbb{Z}[\sqrt{-d}]$ 虽为整环,未必为

Dedekind 环)。

(i) $d \equiv 3 \pmod 8$ 时,$\frac{1}{4}(1+d) \equiv 1 \pmod 2$(注意 d 可表为 $d=8k+3$),在 $R_1=\{0,1\}$ 上 x^2+x+1 不可约,而 $\alpha^2=\alpha-(1+d)/4$,

$$\alpha^2-\alpha+\frac{1}{4}(1+d)=\alpha^2+\alpha+1=0。$$

因此 S 为域,于是 $\mathrm{K}_0(S)\simeq \mathrm{K}_0(R_1)\simeq \mathbb{Z}$,$\mathrm{Pic}(S)\simeq \mathrm{Pic}(R_1)=1$。又由 R_1 为 2 元域,S 为 4 元域知 $\mathrm{K}_1(R_1)\simeq R_1^{\cdot}=1$,$\mathrm{K}_1(S)\simeq S^{\cdot}\simeq \mathbb{Z}_3$。

$d=3,11,19$(见 §23,例 1)时 $R_2\in$ UFD 且为 Dedekind 环,因此为 PID,$\mathrm{K}_0(R_2)\simeq \mathbb{Z}$,$\mathrm{Pic}(R_2)=1$。

(a) $d=3$ 时,取 a 使 $\alpha^2=a\alpha+b$,$a,b\in \mathbb{Z}$。解 Pell 方程 $x^2-ay^2=\pm 1$(可逆元的范必为 ± 1),可得 $R_2^{\cdot}\simeq \mathbb{Z}_6$,$R^{\cdot}\simeq \mathbb{Z}_2$。于是由命题 24.3 得交换图(行正合)

$$\begin{array}{ccccccccccc}
\mathrm{K}_1(R) & \xrightarrow{f_1} & \mathrm{K}_1(R_2) & \xrightarrow{g_1} & \mathbb{Z}_3 & \xrightarrow{\delta} & \mathrm{K}_0(R) & \xrightarrow{f_0} & \mathbb{Z}\oplus\mathbb{Z} & \xrightarrow{g_0} & \mathbb{Z} \\
\downarrow{\scriptstyle \det} & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow{\scriptstyle \det} \\
\mathbb{Z}_2 & \xrightarrow{f_1} & \mathbb{Z}_6 & \xrightarrow{g_1} & \mathbb{Z}_3 & \xrightarrow{\delta} & \mathrm{Pic}(R) & \longrightarrow & 0 & \longrightarrow & 0
\end{array}$$

下行中,$\underline{f_1}\neq 0\Rightarrow \underline{f_1}$ 单 $\Rightarrow \mathrm{Ker}\,\underline{g_1}=\mathrm{Im}\,\underline{f_1}\simeq \mathbb{Z}_2\Rightarrow \underline{g_1}$ 满 $\Rightarrow \underline{\delta}=0$,于是 $\mathrm{Pic}(R)=1$,由 $\underline{g_1}$ 满又可看出上行的 g_1 满,于是 $\delta=0$。由此可知 $\mathrm{K}_0(R)\simeq \mathbb{Z}$。

(b) $d=11,19$ 时,仿上得

$R_2^{\cdot}\simeq R^{\cdot}\simeq \mathbb{Z}_2$,$R_1$,$S$ 同(a),(a)中的交换图中下行的 $\mathbb{Z}_6$ 改为 $\mathbb{Z}_2$ 即得本情况下的行正合交换图。于是下行中 $\underline{f_1}\neq 0\Rightarrow \underline{f_1}$ 为同构 $\Rightarrow \underline{f_1}$ 满 $\Rightarrow \underline{g_1}=0\Rightarrow \underline{\delta}$ 为同构。因此 $\mathrm{Pic}(R)\simeq \mathbb{Z}_3$,而由 $\underline{g_1}=0$ 又可得上行的 $g_1=0$。于是上行的 δ 为单同态,且可看出 $\mathrm{Im} f_0=\mathbb{Z}$。因此 $\mathrm{K}_0(R)\simeq \mathbb{Z}\oplus\mathbb{Z}_3$。

(ii) $d\equiv 7 \pmod 8$ 时,$\frac{1}{4}(d+1)\equiv 0 \pmod 2$,因此 S 中 $\alpha^2=\alpha$,由此知 $S\simeq \mathbb{Z}_2\oplus\mathbb{Z}_2$,$\mathrm{K}_0(S)\simeq \mathbb{Z}\oplus\mathbb{Z}$,$\mathrm{Pic}(S)=1$,$\mathrm{K}_1(S)\simeq S^{\cdot}=1$。

当 $d=7,15,23,31$ 时,R_2 为 Dedekind 环,容易由命题 23.5 看出

$$\mathrm{Cl}(R_2)\simeq \mathrm{Pic}(R_2)\simeq \begin{cases} 1, & d=7 \\ \mathbb{Z}_2, & d=15 \\ \mathbb{Z}_3, & d=23,31 \end{cases}$$

于是 $\mathrm{K}_0(R_2)\simeq \mathbb{Z}\oplus\mathrm{Pic}(R_2)$。而 $R_1\simeq \mathbb{Z}_2$,$\mathrm{K}_0(R_1)\simeq \mathbb{Z}$,$\mathrm{Pic}(R_1)=1$。于是由命题 24.3 得行正合交换图

$$
\begin{array}{ccccccccccc}
K_1(R) & \xrightarrow{f_1} & K_1(R_2) & \xrightarrow{g_1} & 0 & \xrightarrow{\delta} & K_0(R) & \xrightarrow{f_0} & \mathbb{Z}\oplus(\mathbb{Z}\oplus \mathrm{Pic}(R_2)) & \xrightarrow{g_0} & \mathbb{Z}\oplus\mathbb{Z} \\
\downarrow{\scriptstyle \det} & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow{\scriptstyle \det} \\
\mathbb{Z}_2 & \xrightarrow[f_1]{} & \mathbb{Z}_2 & \xrightarrow[g_1]{} & 0 & \xrightarrow[\delta]{} & \mathrm{Pic}(R) & \xrightarrow[f_0]{} & \mathrm{Pic}(R_2) & \xrightarrow[g_0]{} & 0
\end{array}
$$

由此知,下行中f_0为同构。于是 $\mathrm{Pic}(R)\simeq\mathrm{Pic}(R_2)$(由上)已经求出,又由上行知 f_0 是单的,由此可看出 $K_0(R)\simeq\mathbb{Z}\oplus\mathrm{Pic}(R)\simeq\mathbb{Z}\oplus\mathrm{Pic}(R_2)$。 □

注② 由上知,$d=3,7,11,15,19,23,31$ 时,虽然 $R=\mathbb{Z}[\sqrt{-d}]$未必为 Dedekind 环(如 $d=3,7$ 时)但 K_0 群都可分解为 $K_0(R)\simeq\mathbb{Z}\oplus\mathrm{Pic}(R)$。事实上,在这些情况下它们都是 Dedekind 环 $R_2=\mathbb{Z}[\frac{1}{2}(1+\sqrt{-d})]$的真子环,对二次域的代数整元环的真子环 O',可以证明:O'必为 Noether 整环且 $\{O\}\cup\mathrm{Max}O'=\mathrm{Spec}O'$。因此 O'为 Dedekind 环$\Leftrightarrow O'$为整闭的。还需注意的是,对 Dedekind 环 R,$R\in\mathrm{PID}\Leftrightarrow K_0(R)\simeq\mathbb{Z}(\Leftrightarrow R\in\mathrm{UFD})$。但对整环 R,不能由 $K_0(R)\simeq\mathbb{Z}$ 断言 $R\in\mathrm{PID}$,因而为 Dedekind 环,比如域 F 上的多元多项式环 $R=F[x_1,x_2,\cdots,x_n]$,$n>1$。R 为整环,且 $K_0(R)\simeq\mathbb{Z}$,但 R 显然不是 Dedekind 环。

作为本节的结束,建议读者在推论 24.2 中取 $\alpha=\sqrt{-d}$,d 是无平方因子的正整数,或取 $d\equiv1,2(\mathrm{mod}\ 4)$对推论 24.3 研究相关的 Picard 群及 K_0 群的计算,这将会加深对本节方法的理解。

第六章　K_2 群的计算与应用

由于 K_2 群计算的复杂性以及在代数数论中有重要应用，在本章中我们用七节的篇幅进一步地介绍 K_2 群的计算以及一些相对 K 群的计算。特别是在§26 末给出了一个附录，专门介绍数域的 K_2 群研究至今为止(包括了 2001 年的一些新结果)的一些热门问题进展情况。在本章中，我们用 Steinberg 符号$\{,\}$证明了：域 F 的 K_2 群 $K_2F=\langle\{F^{\cdot},F^{\cdot}\}\rangle$，且 F 不可数等价于 K_2F 不可数；当 F 为有限域时，K_2F 是平凡的。对有基本重要性的有限环$\mathbb{Z}_n$，证明了 $K_2\mathbb{Z}_n\simeq\mathbb{Z}_2$($n$ 为 4 的倍数时)或平凡群(n 非 4 的倍数时)。用符号$\langle,\rangle$则给出了交换局部环的 K_2 群的生成系，并将这一结果推广到一类重要的交换环(见推论 30.5)。§27 较详细地介绍了研究 K_2 群用到的重要工具——赋值，并给出有理数域$\mathbb{Q}$的 K_2 群的结构分解的优美结果。§28 还给出了由 Steinberg 符号导出的一些互反律，特别是数论中常用的二次互反律。在§31 中，我们还证明了 $K_2\mathbb{Z}\simeq\mathbb{Z}_2$。如果将$\mathbb{Z}$看作是$\mathbb{Z}_0=\mathbb{Z}/0\mathbb{Z}$，这与 $K_2\mathbb{Z}_n$(n 为 4 的倍数时)的上述结果是一致的。

§25　Steinberg 符号与 K_2 群的计算

由于 K_2 群的计算较为复杂，在研究 K_2 群时，常用的方法是(利用一些便于演算的符号)找出 K_2 群的一些元素(研究这些元素的阶常可得到 K_2 群的一些子群)或子群(Sylow p-子群等)。比如，在 $E(R)$中若找到 A,B 使 $AB=BA$。取它们在 Steinberg 映射 $\phi:St(R)\twoheadrightarrow E(R)$下的原象 $a,b\in St(R)$(即 $\phi(a)=A,\phi(b)=B$)。由 $K_2(R)=\mathrm{Ker}\phi$ 即知$[a,b]\in K_2(R)$。在这种情

况下,J. Milnor 引进了记号 $A*B=[a,b]$(其中 $\phi(a)=A,\phi(b)=B$)。在§11 中我们事实上已经得到(见引理 11.1)。

引理 25.1　设 $A,B\in E(R),AB=BA,a,b\in St(R)$ 使 $\phi(a)=A,\phi(b)=B$,则 $A*B\in K_2(R)$与 a,b 的选取无关。

证　由 $K_2(R)=\mathrm{Ker}\phi=C(St(R))$知,若又有 $\phi(a_1)=A,\phi(b_1)=B$,则有 $c,d\in C(St(R))$使 $a_1=ac,b_1=bd$,于是$[a_1,b_1]=[a,b]=A*B$。　□

再来证明 * 运算的一些规律(事实上是换位子性质与 K_2 群定义的结合)。

引理 25.2　(1) 若 $A,B\in E(R)$使 $AB=BA$,则 $B*A=(A*B)^{-1}$(反对称性);

(2) 若 $A,B,A_1,A_2,B_1,B_2\in E(R)$使 $A_jB=BA_j,AB_j=B_jA,j=1,2$,则

$$(A_1A_2)*B=(A_1*B)(A_2*B),$$
$$A*(B_1B_2)=(A*B_1)(A*B_2)\text{(双线性性(双乘性))};$$

(3) 设 $A,B\in E(R)$使 $AB=BA$,则

$(PAP^{-1})*(PBP^{-1})=A*B,\ \forall P\in E(R)$(内自同构下的不变性)。

证　(1) 由$[b,a]=[a,b]^{-1}$即得。

(2) 取 a_1,a_2,b 分别为 A_1,A_2,B 在 ϕ 下的原象,则

$$(A_1*B)(A_2*B)=a_1b_\wedge a_1^{-1}\underline{b^{-1}a_2ba_2^{-1}}b^{-1}$$

(横线上元素 $\in K_2(R)=C(St(R))$,可换到 $\wedge$ 处)

$$=a_1a_2ba_2^{-1}a_1^{-1}b^{-1}=(A_1A_2)*B$$

$$A*(B_1B_2)\overset{}{\underset{(1)}{=\!=}}((B_1B_2)*A)^{-1}$$
$$=((B_1*A)(B_2*A))^{-1}=(B_2*A)^{-1}(B_1*A)^{-1}$$
$$\underset{(1)}{=\!=}(A*B_2)(A*B_1)\underset{K_2(R)\in AG}{=\!=\!=}(A*B_1)(A*B_2)$$

(3) 令 $\phi(p)=P,\phi(a)=A,\phi(b)=B$,则

$$(PAP^{-1})*(PBP^{-1})=pap^{-1}pbp^{-1}pa^{-1}p^{-1}pb^{-1}p^{-1}$$
$$=_\wedge p\underline{aba^{-1}b^{-1}}p^{-1}=[a,b]=A*B$$　□

E(R)中的下述元素

$$d_{12}(u)=\begin{pmatrix}u&&&\\&u_1^{-1}&&\\&&1&\\&&&I_\infty\end{pmatrix},$$

$$d_{13}(v)=\begin{pmatrix} v & & & \\ & 1 & & \\ & & v^{-1} & \\ & & & I_\infty \end{pmatrix},\quad \begin{matrix} u,v\in R^{\cdot}, \\ uv=vu, \end{matrix}$$

特别有用，因为容易看出 $d_{12}(u)d_{13}(v)=d_{13}(v)d_{12}(u)$。故 $d_{12}(u)*d_{13}(v)\in K_2(R)$。对此，我们给出定义

定义 25.1 设 $R\in \mathcal{R}\mathrm{ing}$，$u,v\in R^{\cdot}$ 使 $uv=vu$，记

$$\{u,v\}=d_{12}(u)*d_{13}(v)$$

称$\{,\}$为 **Steinberg 符号**。

注① Steinberg 符号作用很大，可以证明：若 $R\in \mathcal{C}\mathrm{Ring}$ 且有环同态 $R\to\mathbb{C}$(复数域)，x,y 为不定元，则$\{x,y\}$生成 $K_2(R[x,y,x^{-1},y^{-1}])$的一个无限循环的直和项(见[Milnor,1971])。另一方面，Steinberg 符号又是研究域的 K_2 群(特别是数域的代数整元环的 K_2 群)的主要工具之一。

Steinberg 符号有如下的便于计算的性质

定理 25.1 设 $R\in \mathcal{R}\mathrm{ing}$，$u,u_j,v,v_j\in R^{\cdot}$ 且 $uv_j=v_ju$，$u_jv=vu_j$，$j=1,2$，则 Steinberg 符号具有如下的基本性质(1)，(2)，(3)以及导出性质(4)，…，(9)：

(1) $\{u,v\}=\{v,u\}^{-1}$(反对称性)；

(2) $\{u_1u_2,v\}=\{u_1,v\}\{u_2,v\}$，

$\{u,v_1v_2\}=\{u,v_1\}\{u,v_2\}$(双乘性)；

(3) 当 $1-u\in R^{\cdot}$ 时，$\{u,1-u\}=1$(即 $u+v=1$ 时，$\{u,v\}=1$)；

(4) $\{u,1\}=\{1,v\}=1$；

(5) $\{u,-u\}=1$；

(6) $\{u,u\}^2=1$；

(7) $\{u,-1\}^2=\{-1,v\}^2=1$；

(8) $\{u^{-1},v\}=\{u,v^{-1}\}=\{u,v\}^{-1}=\{v,u\}$；

(9) 若 $2\in R^{\cdot}$，则$\{2^n,-1\}=1$，$\forall n\in\mathbb{N}$。

证 (1)，(2)由定义 25.1 与引理 25.2 即得。

(3) 在下面引进一些记号与工具后再证(用不到这里的(4)，…，(9)!)。

(4) $\{u,1\}=\{u,1\cdot 1\}\overset{}{\underset{(2)}{=\!=}}\{u,1\}\{u,1\}$，消去$\{u,1\}$即得$\{u,1\}=1$。

$\{1,v\}\underset{(1)}{=\!=}\{v,1\}^{-1}=1^{-1}=1$。

(8) 由$\{u^{-1},v\}\{u,v\}=\{1,v\}=1$ 知$\{u^{-1},v\}=\{u,v\}^{-1}=\{v,u\}$，同理知$\{u,v^{-1}\}=\{u,v\}^{-1}$。

(5) $u=1$ 时由(4)知$\{u,-u\}=1$；$u\neq 1$ 时，注意 $1-u^{-1}=-u^{-1}(1-u)$。于是当 $1-u\in R^{\cdot}$ 时 $-u=(1-u)(1-u^{-1})^{-1}$，$\{u,-u\}=\{u,(1-u)(1-u^{-1})^{-1}\}\overset{}{\underset{(2)}{=\!=}}\{u,1-u\}\{u,(1-u^{-1})^{-1}\}\underset{(8)}{=\!=}\{u,1-u\}\{u^{-1},1-u^{-1}\}$。因此，在这种情况下，(5)的证明也归为(3)的证明。用后面的引理 25.5 与引理 25.4 的(4)，(5)，可对一般情况(不限 $1-u\in R^{\cdot}$)证明(5)。

(6) 由(1)知，$\{u,u\}=\{u,u\}^{-1}$，即$\{u,u\}^2=1$。

(7) $\{u,-1\}^2\underset{(2)}{=\!=}\{u,1\}=1$，同理知$\{-1,v\}^2=1$。

(9) 由(3)可知$\{2,-1\}=1$，因此$\{2^n,-1\}=1$(由(2))。 □

注②　事实上定理中的(2)，(3)为基本性质，(1)也可由(2)，(3)推出。因为用后面将(不用(1))推出的(5)及由(2)推出的(8)可得

$$
\begin{aligned}
\{u,v\} &= \{u,v\}\{u,-u\} \\
&= \{u,-vu\} = \{u,-vu\}\{vu,-vu\}^{-1} \\
&= \{u,-vu\}\{u^{-1}v^{-1},-vu\} = \{v^{-1},-vu\} \\
&= \{v^{-1},-v^{-1}\}\{v^{-1},-vu\} = \{v^{-1},u\} \\
&= \{v,u\}^{-1}
\end{aligned}
$$

注意上述的

$$
\begin{aligned}
d_{12}(u) &= e_{12}^{u}e_{21}^{-u^{-1}}e_{12}^{u}e_{12}^{-1}e_{21}^{1}e_{12}^{-1}, \\
d_{13}(v) &= e_{13}^{v}e_{31}^{-v^{-1}}e_{13}^{v}e_{13}^{-1}e_{31}^{1}e_{13}^{-1}。
\end{aligned}
$$

据此，可引进记号

$$
\begin{aligned}
w_{ij}(u) &= x_{ij}(u)x_{ji}(-u^{-1})x_{ij}(u), \\
h_{ij}(u) &= w_{ij}(u)w_{ij}(-1), \qquad \forall u\in R^{\cdot}, i\neq j
\end{aligned} \tag{1}
$$

于是

$$
\begin{aligned}
d_{12}(u) &= \phi(h_{12}(u)), \\
d_{13}(v) &= \phi(h_{13}(v)),\ \{u,v\} = [h_{12}(u),h_{13}(v)]
\end{aligned} \tag{2}
$$

先来证，更一般地有

引理 25.3　设 $R\in$ Ring，$u\in R^{\cdot}$，$i\neq j$，则 $w_{ij}(u)w_{ij}(-u)=1$，即，$(w_{ij}(u))^{-1}=w_{ij}(-u)$，因此 $h_{ij}(1)=1$。

证　$w_{ij}(u)w_{ij}(-u)$

$$
\begin{aligned}
&= x_{ij}(u)x_{ji}(-u^{-1})\underline{x_{ij}(u)\cdot x_{ij}(-u)}x_{ji}(u^{-1})x_{ij}(-u) \\
&= x_{ij}(u)\underline{x_{ji}(-u^{-1})x_{ji}(u^{-1})}x_{ij}(-u) \\
&= x_{ij}(u)x_{ij}(-u)=1
\end{aligned}
$$
□

下面为方便起见，将$(w_{ij}(u))^{-1}$记为 $w_{ij}(u)^{-1}$我们有

引理 25.4 设 $R\in\mathrm{Ring}, u,v\in R^{\cdot}$，则

(1) 若 i,j,k,l 互异，则

$$w_{ij}(v)x_{kl}(u) = x_{kl}(u)w_{ij}(v),$$
$$w_{ij}(v)w_{kl}(u) = w_{kl}(u)w_{ij}(v),$$

于是

$$w_{kl}(u)x_{ij}(v)w_{kl}(u)^{-1} = x_{ij}(v),$$
$$w_{kl}(u)w_{ij}(v)w_{kl}(u)^{-1} = w_{ij}(v);$$

(2) 若 i,j,l 互异，则

$$w_{il}(u)x_{ij}(v)w_{il}(u)^{-1} = x_{lj}(-u^{-1}v),$$
$$w_{il}(u)x_{ji}(-v^{-1})w_{il}(u)^{-1} = x_{jl}(v^{-1}u),$$

因此

$$w_{il}(u)w_{ij}(v)w_{il}(u)^{-1} = w_{lj}(-u^{-1}v);$$

(3) 若 i,j,l 互异，则

$$w_{jl}(u)w_{ij}(v)w_{jl}(u)^{-1} = w_{il}(-vu),$$
$$w_{ij}(u)w_{lj}(v)w_{ij}(u)^{-1} = w_{li}(u)^{-1};$$

(4) 若 $i\neq j$，则

$$w_{ij}(u)w_{ij}(v)w_{ij}(u)^{-1} = w_{ji}(-u^{-1}vu^{-1}),$$
$$w_{ij}(u)x_{ij}(v)w_{ij}(u)^{-1} = x_{ji}(-u^{-1}vu^{-1});$$

(5) $w_{ij}(u)=w_{ji}(-u^{-1})$。

证 由 $\{x_{ij}(a)\}$ 的 Steinberg 关系（(S_1)，(S_2)，(S_3) 见 § 10）知(1)是显见的。

(2) $w_{il}(u)x_{ij}(v)w_{il}(u)^{-1}$

$$\overset{\text{def}}{=\!=\!=} x_{il}(u)x_{li}(-u^{-1})\underline{x_{il}(u)x_{ij}(v)}x_{il}(-u)x_{li}(u^{-1})x_{il}(-u)$$

$$\overset{(S_2)}{=\!=\!=} x_{il}(u)x_{li}(-u^{-1})x_{ij}(v)x_{li}(u^{-1})_{\wedge}x_{il}(-u)$$

（$\wedge$ 处填入 $1=x_{ij}(-v)x_{ij}(v)$）

$$= x_{il}(u)[x_{li}(-u^{-1}),x_{ij}(v)]x_{ij}(v)x_{il}(-u)$$

$$\overset{(S_3)}{=\!=\!=} x_{il}(u)x_{lj}(-u^{-1}v)x_{ij}(v)x_{il}(-u)$$

$$\overset{(S_2)}{=\!=\!=} x_{il}(u)x_{lj}(-u^{-1}v)x_{il}(-u)x_{ij}(v)$$

（$\wedge$ 处填入 $x_{il}(-u)x_{lj}(u^{-1}v)x_{lj}(-u^{-1}v)x_{il}(u)=1$）

$$\overset{(S_3)}{=\!=\!=} x_{ij}(u(-u^{-1}v))x_{lj}(-u^{-1}v)x_{ij}(v)$$

$$= x_{ij}(-v)_{\wedge}x_{lj}(-u^{-1}v)\underline{x_{ij}(v)}$$

$=x_{lj}(-u^{-1}v)$

类似地,有

$$w_{il}(u)x_{ji}(-v^{-1})w_{il}(u)^{-1}\xlongequal[\text{def}]{}x_{il}(u)x_{li}(-u^{-1})x_{il}(u)$$

$$x_{ji}(-v^{-1})x_{il}(-u)_{\wedge}x_{li}(u^{-1})x_{il}(-u)$$

(∧处填入 $x_{ji}(v^{-1})x_{ji}(-v^{-1})=1$ 向左凑成换位子)

$=x_{il}(u)x_{li}(-u^{-1})[x_{ji}(-v^{-1}),x_{il}(u)]^{-1}x_{ji}(-v^{-1})x_{li}(u^{-1})x_{il}(-u)$

$=x_{il}(u)x_{li}(-u^{-1})(x_{jl}(-v^{-1}u))^{-1}_{\wedge}x_{ji}(-v^{-1})\underline{x_{li}(u^{-1})}x_{il}(-u)$

$=x_{il}(u)x_{li}(-u^{-1})x_{jl}(v^{-1}u)x_{li}(u^{-1})x_{ji}(-v^{-1})x_{il}(-u)$

$=x_{il}(u)[x_{li}(-u^{-1}),x_{jl}(v^{-1}u)]x_{jl}(v^{-1}u)x_{ji}(-v^{-1})x_{il}(-u)$

$=x_{il}(u)[x_{jl}(v^{-1}u),x_{li}(-u^{-1})]^{-1}x_{jl}(v^{-1}u)x_{ji}(-v^{-1})x_{il}(-u)$

$=x_{il}(u)x_{ji}(v^{-1})_{\wedge}x_{jl}(v^{-1}u)\underline{x_{ji}(-v^{-1})}x_{il}(-u)$

$=x_{il}(u)_{\wedge}x_{jl}(v^{-1}u)\underline{x_{il}(-u)}$

$=x_{jl}(v^{-1}u)$

将这两个结果组合起来,即得(2)中第三式与(3)中第一式。

类似地可证 $w_{ij}(u)x_{lj}(v)w_{ij}(u)^{-1}=x_{li}(vu^{-1})$,并由此得出(3)中的第二式。

(4) 由(2)之第三式知

$$w_{il}(-1)w_{ij}(v)w_{il}(1)=w_{lj}(-(-1)^{-1}v)=w_{lj}(v)$$

于是

$$w_{ij}(v)=w_{il}(1)w_{lj}(v)w_{il}(-1)$$

$$w_{ij}(u)w_{ij}(v)w_{ij}(u)^{-1}=w_{ij}(u)w_{il}(1)w_{lj}(v)w_{il}(-1)w_{ij}(u)^{-1}$$

$$=\underline{w_{ij}(u)w_{il}(1)w_{ij}(u)^{-1}}$$

$$\underline{w_{ij}(u)w_{lj}(v)w_{ij}(u)^{-1}}\ \underline{w_{ij}(u)w_{il}(-1)w_{ij}(u)^{-1}}$$

$$\xlongequal[(2),(3)]{}w_{jl}(-u^{-1})w_{li}(vu^{-1})w_{jl}(u^{-1})$$

$$\xlongequal[(2)]{}w_{ji}(-u^{-1}vu^{-1})$$

另一等式用(2)中第一式类似可证。

(5) 由(4)取 $u=v$ 即得。 □

用类似于引理 25.4 的证法,可得在各种情况下的如下结果。

推论 25.1 设 $R\in$ Ring,$u,v\in R^{*}$,则 $w_{kl}(u)x_{ij}(v)w_{kl}(u)^{-1}$ 与 $w_{kl}(u)w_{ij}(v)w_{kl}(u)^{-1}$ 在各种情况下的值可列如下表:

k,l,i,j 的关系		$w_{kl}(u)x_{ij}(v)w_{kl}(u)^{-1}$	$w_{kl}(u)w_{ij}(v)w_{kl}(u)^{-1}$
k,l,i,j 互异		$x_{ij}(v)$	$w_{ij}(v)$
k,i,j 互异	$l=i$	$x_{kj}(uv)$	$w_{kj}(uv)$
	$l=j$	$x_{ik}(vu^{-1})$	$w_{ik}(vu^{-1})$
l,i,j 互异	$k=i$	$x_{lj}(-u^{-1}v)$	$w_{lj}(-u^{-1}v)$
	$k=j$	$x_{il}(-vu)$	$w_{il}(-vu)$
$k=i,l=j$		$x_{ji}(-u^{-1}vu^{-1})$	$w_{ji}(-u^{-1}vu^{-1})$
$k=j,l=i$		$x_{ji}(-uvu)$	$w_{ji}(-uvu)$

由(2)的第一式取 $u=-1$ 又可得

推论 25.2 设 $R\in$ Ring, $v\in R$, i,j,l 互异，则

$$x_{ij}(v)=w_{il}(1)x_{lj}(v)w_{il}(1)^{-1}$$

下面证明用于证明定理 25.1(3)的关键引理。

引理 25.5 设 $R\in$ Ring, $u,v\in R^{\cdot}$ 且 $uv=vu$，则

$$h_{12}(uv)=h_{12}(u)h_{12}(v)\{u,v\}^{-1}$$

因此 $\{u,v\}=1\Leftrightarrow h_{12}(uv)=h_{12}(u)h_{12}(v)$。

证 由式(2)知

$$\begin{aligned}
\{u,v\} &= [h_{12}(u),h_{13}(v)] \\
&= h_{12}(u)h_{13}(v)h_{12}(u)^{-1}h_{13}(v)^{-1} \\
&\overset{}{\underset{\text{def}}{=\!=\!=}} h_{12}(u)w_{13}(v)\,\underline{w_{13}(-1)w_{12}(1)w_{12}(-u)w_{13}(1)}\,w_{13}(-v) \\
&\underset{\text{引理 25.4(2)}}{=\!=\!=\!=\!=} h_{12}(u)\,\underline{w_{13}(v)w_{32}(1)w_{32}(-u)w_{13}(-v)} \\
&\underset{\text{推论 25.1}}{=\!=\!=\!=\!=} h_{12}(u)w_{12}(v)w_{12}(-vu) \\
&= h_{12}(u)w_{12}(v)w_{12}(-1)w_{12}(1)w_{12}(-vu) \\
&= h_{12}(u)h_{12}(v)h_{12}(vu)^{-1} \\
&= h_{12}(u)h_{12}(v)h_{12}(uv)^{-1}
\end{aligned}$$

于是欲证之式成立(注意 $\{u,v\}\in K_2(R)=C(\mathrm{St}(R))$)。 □

[定理 25.1(3)($\{u,1-u\}=1,\forall u\in R^{\cdot}$ 使 $1-u\in R^{\cdot}$)之证]。

由引理 25.5 知，只需证

$$h_{12}(u)h_{12}(1-u)=h_{12}(u-u^2)$$

但由 h_{ij} 的定义知

$$h_{12}(u)h_{12}(1-u)=w_{12}(u)w_{12}(-1)w_{12}(1-u)w_{12}(-1),$$

$$h_{12}(u-u^2)=w_{12}(u-u^2)w_{12}(-1)。$$

因此，只需证明

$$w_{12}(u)w_{12}(-1)w_{12}(1-u)=w_{12}(u-u^2)=w_{12}(uv),$$

其中 $v=1-u$。

事实上，

$$
\begin{aligned}
& w_{12}(u)w_{12}(-1)w_{12}(1-u) = w_{12}(u)w_{21}(1)w_{12}(v) \\
&\quad = w_{12}(u)x_{21}(1)x_{12}(-1)x_{21}(1)w_{12}(v) \\
&\quad = \underline{w_{12}(u)x_{21}(1)w_{12}(-u)}w_{12}(u)x_{12}(-1) \\
&\qquad w_{12}(v)\ \underline{w_{12}(-v)x_{21}(1)w_{12}(v)} \\
&\quad \xlongequal[\text{推论 25.1}]{} x_{12}(-u^2)w_{12}(u)x_{12}(-1)w_{12}(v)x_{12}(-v^2) \\
&\quad \xlongequal[\text{def}]{} x_{12}(-u^2)x_{12}(u)x_{21}(-u^{-1})x_{12}(u) \\
&\qquad x_{12}(-1)x_{12}(v)x_{21}(-v^{-1})x_{12}(v)x_{12}(-v^2) \\
&\quad = x_{12}(-u^2+u)x_{21}(-u^{-1})x_{12}(0)x_{21}(-v^{-1})x_{12}(v-v^2) \\
&\quad = x_{12}(uv)x_{21}(-u^{-1}-v^{-1})x_{12}(uv) \\
&\quad = w_{12}(uv)(\text{注意 } u+v=1 \Rightarrow u^{-1}+v^{-1}=(uv)^{-1})
\end{aligned}
$$
□

注② 由引理 25.4 可直接验证：引理 25.5 中的 1,2 改为 $i,j(i\neq j)$ 仍成立。由此知，(2)式中 $\{u,v\}$ 的表示式与所用的足码无关。

Steinberg 符号对有限域（q 元域记为 $\mathbb{F}_q$）的平凡性可由下述命题猜出。在下节证出：对任意域，F，$K_2(F)=\{F^*,F^*\}$ 后即知：有限域的 K_2 群都是平凡的。

命题 25.1 对任意的有限域 $\mathbb{F}_q$，$\{\mathbb{F}_q^*,\mathbb{F}_q^*\}=1$。

证 注意 $\mathbb{F}_q^*$ 为 $q-1$ 阶乘法群，可记 $\mathbb{F}_q^*=\{1,u,\cdots,u^{q-2}\}$，只需证 $\{u,u\}=1$，但由定理 25.1 知 $\{u,u\}^2=1$，因此只需再证有奇数 k 使 $\{u,u\}^k=1$。

(1) 当 $2|q$ 时，$q-1$ 为奇数，$\{u,u\}^{q-1}=\{u^{q-1},u\}=\{1,u\}=1$，此时欲证成立。

(2) 当 $2\nmid q$ 时，令 $q=2t+1$，则 $|\mathbb{F}_q^*|=2t$。可设 $t>1$（否则 $q=3$，则 $u=-1$，由 $(-1)+(-1)=1$ 即得 $\{-1,-1\}=1$）。$\mathbb{F}_q^*$ 中必有 t 个平方元与 t 个非平方元，去掉 $1=1^2$，则 $\mathbb{F}_q^*\setminus\{1\}$ 含 $t-1$ 个平方元与 t 个非平方元。而由

$$
\begin{gathered}
\mathbb{F}_q^*\setminus\{1\} \underset{1-1}{\leftrightarrow} \mathbb{F}_q^*\setminus\{1\} \\
x \leftrightarrow 1-x
\end{gathered}
$$

知必有 $1\neq x\in\mathbb{F}_q^*$ 使 x 与 $1-x$ 都非平方元，此时必有 $x=u^i$，$1-x=u^j$，i,j 都是奇数，而由定理 25.1 知

$$
1=\{x,1-x\}=\{u,u\}^{ij}。
$$

注意 ij 为奇数即得欲证。 □

如众周知，对$\mathbb{F}_q$，q 可表为 $q=p^n$，其中 p 为素数，更一般地，我们可研究 p^n 元的环$\mathbb{Z}_q$。我们下面来证：当 $2\nmid q$ 或 $2\parallel q$（即 $2|q,2^2\nmid q$）时，对$\mathbb{Z}_q$，上命题的结果仍成立（注意$\mathbb{Z}_m^{\cdot}$ 为$\mathbb{Q}(\xi_m)/\mathbb{Q}$ 的 Galois 群，其中 $m\in\mathbb{N}$，ξ_m 为 m 次本原单位根，对$\mathbb{Z}_m^{\cdot}$ 的研究是有意义的）。为此先证一条引理（为方便不熟悉原根的读者，这里给出直接的证明）。

引理 25.6 设 $q=p^n$，p 为素数，则

（1）$2\nmid p$（即 $2\nmid q$）时，$\mathbb{Z}_q^{\cdot}$ 为 $p^{n-1}(p-1)$阶循环群且

$$\mathbb{Z}_q^{\cdot}\simeq\mathbb{Z}_{p-1}\oplus\mathbb{Z}_{p^{n-1}};$$

（2）$p=2$ 时，

$$\mathbb{Z}_{2^n}^{\cdot}\simeq\begin{cases}\{1\}(\text{平凡的}), & n=1\\ \mathbb{Z}_2, & n=2\\ \mathbb{Z}_2\oplus\mathbb{Z}_{2^{n-2}}, & n\geqslant 3\end{cases}$$

（3）$8\nmid q$ 时，$\mathbb{Z}_q^{\cdot}$ 必为循环群。

证 （1）在 $1,2,\cdots,p^n$ 中与 p 不互素（即为 p 的倍数）的恰为 $p,2p,\cdots,p^{n-1}\cdot p$ 共 p^{n-1}个，因此与 p 互素的（即$\mathbb{Z}_q^{\cdot}$ 中的元素）共 $p^n-p^{n-1}=p^{n-1}(p-1)$个。但$(p-1,p^{n-1})=1$，于是

$$\mathbb{Z}_q^{\cdot}\simeq G_1\oplus G_2,\ |G_1|=p-1,\ |G_2|=p^{n-1}$$

显然 $\forall x\in G_1, x^{p-1}=1$（$G_1$ 的单位元）；$\forall y\in G_2, y^{p^{n-1}}=1$（$G_2$ 的单位元）。由于$(p-1,p^{n-1})=1$，为证（1），只需证 G_1,G_2 都是循环群。

事实上，$n=1$ 时（1）是有限域性质，不必再证。此时可取 m 使$(m,p)=1$，且

$$\mathbb{Z}_q^{\cdot}=\{m+p\mathbb{Z},m^2+p\mathbb{Z},\cdots,m^{p-1}+p\mathbb{Z}\}(\text{互异的元素集})\qquad(3)$$

$n>1$ 时，令 $k=m^{p^{n-1}}$，则$(m,p)=(k,p)=(k,p^n)=1$，因此 $k+p^n\mathbb{Z},m+p^n\mathbb{Z}\in\mathbb{Z}_{p^n}^{\cdot}$，而

$$k^{p-1}=(m^{p^{n-1}})^{p-1}=m^{\varphi(p^n)}\equiv 1(\bmod p^n)(\text{即 Euler 定理}),$$

其中 $\varphi(x)$表为 Euler 函数（表示 $1,2,\cdots,x$ 中与 x 互素的数的个数），由此知 $k+p^n\mathbb{Z}\in G_1$。但 $m^p\equiv m(\bmod p)$，因此

$$k=m^{p^{n-1}}\equiv m(\bmod p)$$

于是由（3）式知，$k+p\mathbb{Z},k^2+p\mathbb{Z},\cdots,k^{p-1}+p\mathbb{Z}$ 互异。由此更可看出：$k+p^n\mathbb{Z},k^2+p^n\mathbb{Z},\cdots,k^{p-1}+p^n\mathbb{Z}$ 互异，因而为 G_1 的全体元素。故 G_1 为循环群（其生成元为 $k+p^n\mathbb{Z}$）。

为证 G_2 也是循环群，可设 $n\geqslant 2$（否则 $G_2=1$ 平凡）且只需反设 G_2 为 t

个 p^{n_i} 阶循环群的直和，$n_i\geqslant 1$。此时在每一直和项中 $x^p\equiv 1(\mathrm{mod}\ p^n)$ 恰有 p 个解。因此 $x^p\equiv 1(\mathrm{mod}\ p^n)$ 在 G_2 中(即在 $\mathbb{Z}_{p^n}^{\cdot}$ 中，因为 $(p-1,p)=1$)恰有 p^t 个解。下面只需证 $t=1$。

事实上，令

$$S=\{s\mid s\in\mathbb{Z}_{p^n}^{\cdot}(\text{即 } 0<s<p^n(\mathrm{mod}\ p^n))\text{ 且 } s^p\equiv 1(\mathrm{mod}\ p^n)\}$$

注意 $\forall s\in S$，s 可表为 $s=1+a_1p+a_2p^2+\cdots+a_{n-1}p^{n-1}$，$0\leqslant a_j<p$。因此 $s\neq 1$ 时总可表为(将 yp^f 后的多次项合并)

$$\begin{aligned}s&=1+yp^f+zf^{f+1}\\&=1+(y+zp)p^f,\quad 1\leqslant f\leqslant n-1,\ 0<y<p,z\geqslant 0\end{aligned}$$

于是

$$\begin{aligned}s^p&=1+\binom{p}{1}(y+zp)p^f+\binom{p}{2}(y+zp)^2p^{2f}\\&\quad+\cdots+(y+zp)^pp^{pf}\\&\equiv 1+yp^{f+1}(\mathrm{mod}p^{f+2})\end{aligned}$$

而 $s^p\equiv 1(\mathrm{mod}p^n)$，若 $f<n-1$，则 $f+2\leqslant n$。由此又知

$$yp^{f+1}\equiv 0(\mathrm{mod}\ p^{f+2})$$

因此 $y\equiv 0(\mathrm{mod}\ p)$，这与前设的 $0<y<p$ 矛盾。故 $f=n-1$，由此知($s=1$ 算在内)，$x^p\equiv 1(\mathrm{mod}\ p^n)$ 在 G_2 中恰有 p 个解。于是 $p^t=p$，即 $t=1$。

(2) 仿(1)知 $|\mathbb{Z}_{2^n}^{\cdot}|=2^{n-1}=\varphi(2^n)$，$n=1,2$ 时(2)显然成立。下设 $n\geqslant 3$，容易看出 $x^2\equiv 1(\mathrm{mod}\ 2^n)$ 在 $\mathbb{Z}_{2^n}^{\cdot}$ 中至少有 4 解：$a_1=1$，$a_2=-1$，$a_3=1+2^{n-1}$，$a_4=-1+2^{n-1}$。因此 $\mathbb{Z}_{2^n}^{\cdot}$ 至少可分解为两个非平凡的循环群之直和。但 $|\mathbb{Z}_{2^n}^{\cdot}|=2^{n-1}$，由此直和分解可知，$\forall x\in\mathbb{Z}_{2^n}^{\cdot}$，$x^{2^{n-2}}\equiv(\mathrm{mod}\ 2^n)$，即对任一奇数 m，$m^{2^{n-2}}\equiv 1(\mathrm{mod}\ 2^n)$(对偶数 m，显然其 mod 2^n 剩余类不在 $\mathbb{Z}_{2^n}^{\cdot}$ 中)。为证(2)，只需找出 $x\in\mathbb{Z}_{2^n}^{\cdot}$ 使 $x^{2^{n-3}}\not\equiv 1\ (\mathrm{mod}\ 2^n)$。

事实上，取 $x=5+2^n\mathbb{Z}$，若 $n=3$，则 $5^{2^{n-3}}=5\not\equiv 1(\mathrm{mod}\ 2^{n-1})$ 但 $5^{2^{n-3}}\equiv 1(\mathrm{mod}\ 2^{n-1})$。令 $f\geqslant 3$ 且 $k(f)=\max\{k\mid 5^{2^{f-3}}\equiv 1(\mathrm{mod}\ 2^k)\}$，则 $k(3)=2$。由此知

$$5^{2^{f-3}}\equiv 1+y2^{k(f)}(\mathrm{mod}\ 2^k),2\nmid y$$

于是

$$\begin{aligned}5^{2^{(f-1)-3}}&=(5^{2^{f-3}})^2=1+y2^{k(f)+1}+y^22^{2k(f)}\\&\qquad(\text{其中 } k(f+1)\geqslant k(f)\geqslant 2,\ \forall f\geqslant 3)\\&=1+z2^{k(f)+1},z=y+2^{k(f)-1}y^2\ \text{为奇数}\end{aligned}$$

于是 $k(f+1)=k(f)+1$。但 $k(3)=2$，由此可推知 $k(f)=f-1$，$\forall f\geqslant 3$。因此

$$5^{2^{n-3}}\not\equiv 1(\mathrm{mod}\ 2^n),\qquad \forall n\geqslant 3$$

这就证出了(2)。

(3)由(1)，(2)即得。 □

由此引理可证

命题 25.2 设 $R=\mathbb{Z}_m$，$2\nmid m$ 或 $2\parallel m$（即 $2|m$ 但 $4\nmid m$），则在 $K_2(R)$ 中，$\{R^\cdot,R^\cdot\}=1$。

证 (1) $R=\mathbb{Z}_{p^n}$，$2\nmid p$，p 为素数时，由上引理（注意 $q=p^n$）知 $R^\cdot$ 为偶数阶循环群。又 R 为局部环，$\mathfrak{m}=p\mathbb{Z}/p^n\mathbb{Z}\in \mathrm{Max}R$. $\pi:R/\mathfrak{m}\to\mathbb{F}_p$ 为标准环同构。$\pi_1:R^\cdot/G_2\to\mathbb{F}_p^\cdot$ 为 π 诱导的群同构，显见 $\pi_1(a+b)=\pi_1(a)+\pi_1(b)$，$\forall a,b\in R^\cdot/G_2$，其中 G_2 即上引理之证中的 G_2。仿命题 25.1 之证的(2)即知$\{R^\cdot,R^\cdot\}=1$（注意$\mathbb{Z}_{p-1}$可视为$\mathbb{F}_q^\cdot$，而$\mathbb{Z}_{p^{n-1}}$为奇数阶群！）。

(2) $2\nmid m$ 时，由中国剩余定理(CRT)知

$$R\simeq\mathbb{Z}_{p_1^{r_1}}\oplus\cdots\oplus\mathbb{Z}_{p_k^{r_k}}\quad p_1,p_2,\cdots,p_k \text{ 为互异的奇素数。}$$

于是

$$R^\cdot\simeq\mathbb{Z}_{p_1^{r_1}}^\cdot\oplus\cdots\oplus\mathbb{Z}_{p_k^{r_k}}^\cdot$$

由(1)即知$\{R^\cdot,R^\cdot\}=1$。

(3) $2\parallel m$ 时，由 CRT 知

$R\simeq\mathbb{Z}_2\oplus\mathbb{Z}_{p_1^{r_1}}\oplus\cdots\oplus\mathbb{Z}_{p_l^{r_l}}$，其中 $p_1,p_2,\cdots,p_l$ 为互异的奇素数。

于是

$$R^\cdot\simeq\mathbb{Z}_{p_1^{r_1}}^\cdot\oplus\cdots\oplus\mathbb{Z}_{p_l^{r_l}}^\cdot$$

由(2)即知$\{R^\cdot,R^\cdot\}=1$。 □

在§31 我们将进一步证明

$$K_2(\mathbb{Z}_m)=\begin{cases}\langle\{-1,-1\}\rangle\simeq\mathbb{Z}_2, & 4\mid m\text{ 时(R. K. Dennis)}\\ 1, & 4\nmid m\text{ 时}\end{cases}$$

这样就完全算出（确定）了 $K_2(\mathbb{Z}_m)$。

对更一般的情况，我们有如下结果

命题 25.3 设 $R\in\mathbb{C}\mathrm{Ring}$，则

(1) 当 $R^\cdot$ 为循环群时，$\{R^\cdot,R^\cdot\}=1$ 或$\langle\{R^\cdot,R^\cdot\}\rangle\simeq\mathbb{Z}_2$，因此$\{\mathbb{Z}^\cdot,\mathbb{Z}^\cdot\}\simeq 1$ 或$\langle\{\mathbb{Z}^\cdot,\mathbb{Z}^\cdot\}\rangle\simeq\mathbb{Z}_2$；

(2) 当 $R=O_F$ 为虚二次域的代数整元环时，$\{O_F^\cdot,O_F^\cdot\}=1$ 或$\langle\{O_F^\cdot,O_F^\cdot\}\rangle\simeq\mathbb{Z}_2$；

(3) 当 $R=O_F$ 为实二次域的代数整元环时,$\{O_F^\cdot, O_F^\cdot\}$ 只有单位元与二阶元。

证 (1) $R^\cdot=(u)$ 为 u 生成的循环群时 $\langle\{R^\cdot, R^\cdot\}\rangle=\langle\{u,u\}\rangle$ 而 $\{u,u\}=\{u,u\}^{-1}$,即 $\{u,u\}^2=1$。注意到 $\mathbb{Z}^\cdot=\{\pm1\}$ 为由 -1 生成的循环群,即知(1)成立。

(2) 由§7 末已知,对虚二次域 $F=\mathbb{Q}(\sqrt{-d})$($d>0$ 无平方因子),

$$O_F^\cdot=\begin{cases}\{\pm1,\pm i\}=(i)\simeq\mathbb{Z}_4, d=-1\text{ 时}\\ \{\pm1,\pm\omega,\pm\omega^2\}=(-\omega^2)\simeq\mathbb{Z}_6, d=-3\text{ 时}\\ \{\pm1\}=(-1)\simeq\mathbb{Z}_2,\quad d<-3\text{ 或 }d=-2\text{ 时}\end{cases}$$

于是由(1)即得(2)。

(3) 对 $F=\mathbb{Q}(\sqrt{d})$($d>0$ 无平方因子),由§7 末知

$$O_F^\cdot=\{\pm u^m\}$$

注意到 $\{u,u\}^2=1$, $\{-u,u\}=1$, $\{-u,-u\}^2=1$, $\{(-u)^m,u^n\}=\{-u,u\}^{mn}=1$, $\{u^m,u^n\}^2=\{u,u\}^{2mn}=1$,即得(3)。 □

注意 $\langle\{O_F^\cdot, O_F^\cdot\}\rangle$ 只是 K_2O_F 的一个子群,$\langle\{O_F^\cdot, O_F^\cdot\}\rangle\simeq\mathbb{Z}_2$(或 1)只能说明 K_2O_F 有子群同构于 $\mathbb{Z}_2$(或 1)。但反过来,若知 $K_2O_F=1$,则可断言 $\{O_F^\cdot, O_F^\cdot\}=1$。

记 O_F 为 $\mathbb{Q}(\sqrt{d})$ 的代数整元环,J. Tate 在 1973 年给出一个方法算出 $d=-1,-2,-3,-11$ 时 $K_2O_F=1$,而 $d=-7,-15$ 时 $K_2O_F\simeq\mathbb{Z}_2$。M. Skalba 于 1989 年前算出 $d=-5,-19$ 时 $K_2O_F=1$。秦厚荣在[秦厚荣,1994]中算出 $d=-6$ 时 $K_2O_F=1$,在[秦厚荣,1996]中算出 $d=-35$ 时 $K_2O_F\simeq\mathbb{Z}_2$。陈胜与游宏在[陈胜,2001]中算出 $d=-43$ 时 $K_2O_F=1$(郭学军在他的博士论文[郭学军,2000]中也独立地算出了这一结果)。

对更一般的 Dedekind 环 R,设其分式域为 F,1969 年 H. Bass 与 J. Tate 得到一个 Abel 群正合列(平凡群记为 0)(其中 $\lambda=\bigoplus_{P\in\mathrm{Spec}R}\lambda_P$,$\lambda_P$ 由 $F^\cdot$ 到 $\mathbb{Z}$ 的且以 R 作赋值环、以 P 作其极大理想的赋值给出):

$$K_2(R)\to K_2(F)\xrightarrow{\lambda}\bigoplus_{P\in\mathrm{Spec}R}K_1(R/P)\to SK_1(R)\to 0$$

当 R 为数域 F 的代数整元环 O_F 时,$\mathrm{Ker}\lambda$ 称为 F 的 **tame 核(驯(顺)核)**。1973 年 D. Quillen 已证出 $\mathrm{Ker}\lambda=K_2(R)$(见[Lam,$1999_2$]),从而实质上已结束了 tame 核的概念。但这一名称仍在习惯地使用.比如 J. Browkin, H. Gangl, 1999 年在 Math. of Computation 68(225), 291—305 上发表的论文标题就是 Tame and wild kernels of quadratic imaginary number fields。

我们在下节将证明 K_2F(F 为域)是由$\{F^{\cdot},F^{\cdot}\}$生成的(事实上还可证:定理 25.1 中的(2),(3)为其关系集)。但具体的结构研究仍十分艰辛,目前仍在进行着。比如[秦厚荣,1994]证明了:若 $\mathrm{Ch}F\neq 2$,则 K_2F 的 4 阶元都可表为$\{a,a^2+1\}\{-1,b\}$,其中 $a,a^2+1,b\in F^{\cdot}$,这是 J. Browkin 1982 年关于$\mathbb{Q}$ 的相应结果的大步推广。

§26 域的 K_2 群及应用

首先注意,对上节定义的 $w_{ij}(u)$($u\in R^{\cdot}$),在 Steinberg 同态 ϕ:St(R)→E(R)下的象

$$\phi(w_{ij}(u)) = e_{ij}^{u}e_{ji}^{-u^{-1}}e_{ij}^{u}$$

$$= \begin{pmatrix} 1 &&&&&&&& \\ & \ddots &&&&&&& \\ && 1 &&&&&& \\ &&& 0 & \cdots & & u && \\ &&&& 1 &&&& \\ &&&&& \ddots &&& \\ &&&&&& 1 && \\ &&& -u^{-1} & \cdots & & 0 && \\ &&&&&&& 1 & \\ &&&&&&&& \ddots \end{pmatrix}$$

$$= P_{ij}\begin{pmatrix} 1 &&&&&&& \\ & \ddots &&&&&& \\ && -u^{-1} &&&&& \\ &&& 1 &&&& \\ &&&& \ddots &&& \\ &&&&& 1 && \\ &&&&&& u & \\ &&&&&&& 1 \\ &&&&&&&& \ddots \end{pmatrix} \qquad (1)$$

其中 P_{ij} 为单位矩阵经第 i 行,第 j 行的交换而来。一般地将单位矩阵的行(列)作置换排成的矩阵称为置换矩阵(它每行,每列都只有一个 1,其余非 1

的元素都为 0），由此可引入一个定义。

定义 26.1　设 $A\in GL_n(R)(GL(R))$ 且 $A=PD$ 或 (DP)，其中 P 为置换矩阵，D 为对角矩阵（等价地，A 每行每列恰有一个非零元）则称 A 为**单项矩阵**（monomial matrix）。若 $x\in St(R)$，则 $\phi(x)$ 为单项矩阵时称 x 为**单项元**（monomial element），$\phi(x)$ 为对角矩阵时称 x 为**对角元**（diagonal element）。

记 $St_n(R)$ 的子群

$$W_n = W_n(R) = \langle\{w_{ij}(R^{\cdot}) \mid 1\leqslant i\neq j\leqslant n\}\rangle,$$

$$H_n = H_n(R) = \langle\{h_{ij}(R^{\cdot}) \mid 1\leqslant i\neq j\leqslant n\}\rangle,$$

$$C_n = C_n(R) = \mathrm{Ker}(\phi\mid_{W_n}) \lhd K_2(R)。$$

不难证明下述命题，其中的（5）将引理 25.4 作了一般化的处理。

命题 26.1　设 $R\in\mathfrak{Ring}$，Steinberg 同态 ϕ: $St(R)\to E(R)$ 在 $St_n(R)$ 上的限制也记为 ϕ，则

（1）$\forall w\in W_n$，$\phi(w)=PD$，其中 P 对应的 $\sigma\in S_n$ 与对角矩阵 D 由 w 惟一确定，称 σ 为由 w 对应的置换。因此，$R\in\mathfrak{CRing}$ 时，$\phi(W_n)=\{B\mid B$ 为单项矩阵且 $\det B=1\}$；

（2）$\phi(w_{ij}(u))=P_{ij}\,\mathrm{diag}(1,\cdots,1,\underset{(i)}{-u^{-1}},1,\cdots,1,\underset{(j)}{u},1,\cdots,1)$，$P_{ij}$ 对应 $(ij)\in S_n$；

（3）$\phi(h_{ij}(u))=I_n\cdot\mathrm{diag}(1,\cdots,1,\underset{(i)}{u},1,\cdots,1,\underset{(j)}{u^{-1}},1,\cdots,1)$，

$=\mathrm{diag}(1,\cdots,1,u,1,\cdots,1,u^{-1},1,\cdots,1)$，$I_n$ 对应恒等置换 $(1)\in S_n$；

（4）$\psi_n: W_n\to S_n$ 为满同态，且 $H_n<\mathrm{Ker}\psi_n\lhd W_n$；

$w_{ij}(u)\mapsto(ij)$

（5）设 $w\in W_n$，$\phi(w)=PD$，其中 P 对应 $\sigma\in S_n$，$D=\mathrm{diag}(u_1,\cdots,u_n)$，则

$$wx_{ij}(v)w^{-1} = x_{\sigma(i)\sigma(j)}(u_ivu_j^{-1}),$$

$$ww_{ij}(v)w^{-1} = w_{\sigma(i)\sigma(j)}(u_ivu_j^{-1}),$$

$$wh_{ij}(v)w^{-1} = h_{\sigma(i)\sigma(j)}(u_ivu_j^{-1})h_{\sigma(i)\sigma(j)}(u_iu_j^{-1})^{-1},$$

因此 $H_n\lhd W_n$；

（6）$h_{ij}(u)h_{ik}(v)h_{ij}(u)^{-1}=h_{ik}(uv)h_{ik}(u)^{-1}$，$\forall u,v\in R^{\cdot}$；

（7）$\{u,v\}=[h_{ij}(u),h_{ik}(v)]=h_{ik}(uv)h_{ik}(u)^{-1}h_{ik}(v)^{-1}$，$\forall u,v\in R^{\cdot}$，$uv=vu$，$i\neq j,k$，即 $\{u,v\}$ 的定义 $\{u,v\}=[h_{12}(u),h_{13}(v)]$ 与足码 1，2，3 无关。

证　（1）$w=w_{ij}(u)$ 时由（1）式知 $\phi(w_{ij}(u))=P_{ij}\,\mathrm{diag}(1,\cdots,1,-u^{-1}$，

$1,\cdots,1,u,1,\cdots)\equiv P_{ij}D_{ij}$，此时(1)当然成立。若 $w=w_{ij}(u)w_{kl}(v)$则

$$\phi(w)=\phi(w_{ij}(u)\phi(w_{kl}(v))=P_{ij}D_{ij}P_{kl}D_{kl}$$
$$=P_{ij}P_{kl}(P_{kl}^{-1}D_{ij}P_{kl})D_{kl}$$

注意 $P_{kl}^{-1}D_{ij}P_{kl}$ 仍为对角矩阵，即知此时(1)仍成立。依此类推即得(1)。

(2) 已由(1)式给出。

(3) 由 $h_{ij}(u)=w_{ij}(u)w_{ij}(-1)$用(1)的证明即得。

(4) 由于任意的 $\sigma\in S_n$ 都可写为对换之积：

$$\sigma=(i_1j_1)(i_2j_2)\cdots(i_kj_k),$$

且对应置换矩阵之积 $P_{i_1j_1}\cdots P_{i_kj_k}$。又由(1)之证知 ψ_n 为群同态，且

$$\phi(w_{i_1j_1}(1)\cdots w_{i_kj_k}(1))=P_{i_1j_1}\cdots P_{i_kj_k}D(D\text{ 为对角矩阵}),$$

即 $\psi_n(w_{i_1j_1}(1)\cdots w_{i_kj_k}(1))=\sigma$。这就证出(4)。

(5) 由(1)及其证明，再用推论 25.1 即得(5)的第一式。

记 $\sigma(i)=s,\sigma(j)=t$，则由(5)中第一式得

$$ww_{ij}(v)w^{-1}=wx_{ij}(v)x_{ji}(-v^{-1})x_{ij}(v)w^{-1}$$
$$=(wx_{ij}(v)w^{-1})(wx_{ji}(-v^{-1})w^{-1})(wx_{ij}(v)w^{-1})$$
$$=x_{st}(u_ivu_j^{-1})x_{ts}(-u_jv^{-1}u_i^{-1})x_{st}(u_ivu_j^{-1})=w_{st}(u_ivu_j^{-1})$$
$$=w_{\sigma(i)\sigma(j)}(u_ivu_j^{-1})$$

即(5)中第二式成立。仿此又有

$$wh_{ij}(v)w^{-1}=ww_{ij}(v)w_{ij}(-1)w^{-1}$$
$$=(ww_{ij}(v)w^{-1})(ww_{ij}(-1)w^{-1})$$
$$=w_{st}(u_ivu_j^{-1})w_{st}(-u_iu_j^{-1})$$
$$=(w_{st}(u_ivu_j^{-1})w_{st}(-1))(w_{st}(1)w_{st}(-u_iu_j^{-1}))$$
$$=h_{st}(u_ivu_j^{-1})h_{st}(u_iu_j^{-1})^{-1}$$
$$=h_{\sigma(i)\sigma(j)}(u_ivu_j^{-1})h_{\sigma(i)\sigma(j)}(u_iu_j^{-1})^{-1}$$

这就证出了(5)中的第三式。

(6) 将 $h_{ij}(u)=w_{ij}(u)w_{ij}(-1)$代入(6)中之式的左端用(5)中的第三式即得。

(7) 由 $h_{ij}(u)=w_{ij}(u)w_{ij}(-1)$用(5)之第三式可得

$$w_{pi}(1)h_{ik}(\alpha)w_{pi}(1)^{-1}=h_{pk}(\alpha)h_{pk}(1)^{-1}=h_{pk}(\alpha),\ \forall\alpha\in R^{\cdot},p\neq i,k$$
$$w_{qk}(1)h_{pk}(\alpha)w_{qk}(1)^{-1}=h_{pq}(\alpha),\ \forall\alpha\in R^{\cdot},\ q\neq p,k$$

取 $p\neq q$ 且 $p,q\neq 1,3,i,k$ 并取

$$w=w_{3q}(1)w_{1p}(1)w_{qk}(1)w_{pi}(1)$$

则 w 对应 $\sigma\in S_n$(n 充分大)且 $\sigma=(3q)(1p)(qk)(pi)$。于是 $\sigma(i)=1,\sigma(k)=3$ 且

$$w(h_{ik}(uv)h_{ik}(u)^{-1}h_{ik}(v)^{-1})w^{-1}$$
$$= h_{13}(uv)h_{13}(u)^{-1}h_{13}(v)^{-1} = \{u,v\}$$

注意 $\{u,v\}\in K_2(R)=C(\mathrm{St}(R))$ 即得(7)。 □

下面为方便起见，使用如下符号

$$C=\bigcup_{n=1}^{\infty}C_n,\ W=\bigcup_{n=1}^{\infty}W_n,\ S=\bigcup_{n=1}^{\infty}S_n,\ H=\bigcup_{n=1}^{\infty}H_n$$

显然 $\psi_n: W_n\to S_n$ 的开拓 $\psi: W\to S$ 仍为满同态且使 $H\subseteq\mathrm{Ker}\psi$，又由 H_n 知 $H\lhd W$，因此 $H\lhd\mathrm{Ker}\psi$。

下面先证两条引理，从而得到 C(作为 $K_2(R)$ 的一个子群)的生成系。

引理 26.1　$\psi: W\to S$ 诱导出群同构 $\bar\psi: W/H\to S$，因此 $H=\mathrm{Ker}\psi\lhd W$。

证　由 ψ 满知

$$S\simeq W/\mathrm{Ker}\psi\simeq(W/H)/(\mathrm{Ker}\psi/H)$$

因此 $\bar\psi$ 为满同态。下面只需证 $\bar\psi$ 单，即证 $\mathrm{Ker}\bar\psi=1$，$\forall w\in W$，记 $\bar w=wH$。由

$$h_{ij}(u)=w_{ij}(u)w_{ij}(-1)=w_{ij}(u)w_{ij}(1)^{-1}\in\mathrm{Ker}\psi$$

知，$\bar w_{ij}(u)=\bar w_{ij}(1)$，$\forall u\in R^{\cdot}$，于是可定义与 u 无关的

$$w_{ij}=\bar w_{ij}(u)=\bar w_{ij}(1)$$

由命题 26.1，可记 $ww_{ij}(u)w^{-1}=w_{kl}(v)$，于是有 $\bar w w_{ij}=w_{kl}\bar w$，其中 $w\in W$ 使 $\psi(w)=\pi=(i\,k)(j\,l)\cdots$。但 $w_{ij}(1)w_{ij}(-1)=1$，因此 $w_{ij}^2=1$。再由 $w_{ij}(u)=w_{ji}(-u^{-1})$ 又知 $w_{ij}=w_{ji}$。令

$$\bar w=w_{i_1j_1}w_{i_2j_2}\cdots w_{i_mj_m},\ n=\max\{i_1,\cdots,i_m,j_1,\cdots,j_m\}$$

由 $w_{ij}=w_{ji}$，不失一般地可设 $i_k<j_k$，$k=1,2,\cdots,m$。记 $r=\min\{k\,|\,j_k=n\}$。

若 $r<m$，由推论 25.1 与 $w_{ij}=w_{ji}$ 知

$\forall j,k\neq n$，必有 p 使 $w_{in}w_{jk}=w_{jk}w_{pn}$(带 n 足码的可调后)；

$\forall i\neq j,i,j\neq n,w_{in}w_{jn}=w_{ji}w_{in}$(使带 n 足码的减少)；

$\forall i\neq n,w_{in}w_{in}=1$(使带 n 足码的成对地减少)。

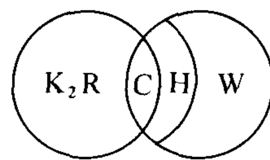
于是用于 $w_{i_kj_k}w_{i_{k+1}j_{k+1}}$ 经有限步必可写成 $\bar w=1$ 或 $r=m$(即足码 n 只出现在最后一个因子)。

当 $r=m$ 时，$\bar\psi(\bar w)=\sigma_1\sigma_2$，其中 $\sigma_1=(i_1j_1)(i_2j_2)\cdots(i_{m-1}j_{m-1})$，$\sigma_2=(i_mj_m)=(i_mn)$。因此 $\sigma_1\in S_{n-1}$，$\sigma_2\notin S_{n-1}$，于是 $\sigma_1\sigma_2\neq1$。由此知 $\bar\psi(\bar w)\neq1$(除非 $\bar w=1$)。故 $\mathrm{Ker}\bar\psi=1$。 □

引理 26.2　(1) $C\lhd H=\langle\{h_{1j}(R^{\cdot})\,|\,j\neq1\}\rangle$；

(2) $K_2(R)\rhd C=K_2(R)\cap W=K_2(R)\cap H\lhd H\lhd W$。

证 （1）显然 $C=K_2(R)\cap W$ 而且 $\forall c\in C$，$\phi(c)=1$。而 $\phi(c)=PD$，其中 P 对应 $\psi(c)$，$D=I$（单位矩阵）。由此知 $\psi(c)=1$，再由引理 26.1 知 $c\in H=\mathrm{Ker}\psi$，于是 $C\lhd H$（注意 $C\subseteq K_2(R)$）。



再证 $H=\langle\{h_{1j}(R^{\cdot})\mid j\neq 1\}\rangle$

$\forall u\in R^{\cdot}$，由 $h_{jk}(u)$ 的定义用命题 26.1 知

$$\begin{aligned}h_{ik}(u)w_{jk}(1)h_{ik}(u)^{-1}&=w_{ik}(u)\underline{w_{ik}(-1)w_{jk}(1)w_{ik}(1)^{-1}}w_{ik}(u)^{-1}\\&=w_{ik}(u)w_{ji}(-1)w_{ik}(u)^{-1}\\&=w_{jk}(u)=h_{jk}(u)w_{jk}(-1)^{-1}\\&=h_{jk}(u)w_{jk}(1)\end{aligned}$$

于是

$$\begin{aligned}h_{jk}(u)&=h_{ik}(u)w_{jk}(1)h_{ik}(u)^{-1}w_{jk}(1)^{-1}\\&=h_{ik}(u)(w_{jk}(1)h_{ik}(u)w_{jk}(1)^{-1})^{-1}=h_{ik}(u)h_{ij}(u)^{-1}\end{aligned}\tag{2}$$

令 $i=1,j,k\neq 1$ 即得

$$h_{jk}(u)=h_{1k}(u)h_{1j}(u)^{-1}$$

于是 $H=\langle\{h_{1j}(R^{\cdot})\mid j\neq 1\}\rangle$。

（2）由（1）知 $C\lhd H$，又 $H\lhd W$，$C=K_2(R)\cap W$，因此（2）成立。 □

由此引理之证的（2）式又得

$$h_{kj}(u)=h_{ij}(u)h_{ik}(u)^{-1}$$

于是有

推论 26.1 设 $R\in\mathbb{R}\mathrm{ing}$，$u\in R^{\cdot}$，则

$$h_{kj}(u)=h_{jk}(u)^{-1}$$

因此 $H=\langle\{h_{j1}(R^{\cdot})\mid j\neq 1\}\rangle$。

现在给出 $K_2(R)$ 的子群 C 的生成系。

命题 26.2 设 $R\in\mathbb{R}\mathrm{ing}$，则

$$C=\langle\{\{u,v\}\mid u,v\in R^{\cdot}\text{ 且 }uv=vu\}\rangle\lhd K_2(R)$$

当 $R\in\mathbb{C}\mathrm{Ring}$ 时，$C=\langle\{R^{\cdot},R^{\cdot}\}\rangle$。

证 记 $C^{*}=\langle\{\{u,v\}\mid u,v\in R^{\cdot}\text{ 且 }uv=vu\}\rangle$。由引理 26.2 知

$$\{u,v\}=[h_{12}(u),h_{13}(v)]\in K_2(R)\cap H=K_2(R)\cap W=C$$

知 $C^{*}<C$。下面只需证 $C^{*}\lhd C$ 且 $C/C^{*}=1$ 即可。

事实上，由 $C^{*}<K_2(R)=C(\mathrm{St}(R))$ 即知 $C^{*}<C(H)$（H 的中心）。由此知 $C^{*}\lhd H$，更有 $C^{*}\lhd C$（注意 $C<H$）。取标准群同态

$$H\twoheadrightarrow H/C^{*},$$

$$h\mapsto\bar{h}$$

由引理 26.2(1)知

$$H/C^* = \langle\{\bar{h}_{1j}(R^\cdot) \mid j \neq 1\}\rangle$$

又由命题 26.1(7)知

$$[h_{1j}(u), h_{1k}(v)] = \{u, v\} \in C^*$$

于是$[\bar{h}_{1j}(u), \bar{h}_{1k}(v)] = \bar{1}$，在命题 26.1(7)中取 $i=1$，又知

$$h_{1k}(uv)h_{1k}(u)^{-1}h_{1k}(v)^{-1} = \{u, v\} \in C^*$$

因此

$$\bar{h}_{1k}(v)\bar{h}_{1k}(u) = \bar{h}_{1k}(uv)$$

于是任意的 $\bar{h} \in H/C^*$ 都可表如下形(注意 $h_{ij}(1)=1, \bar{h}_{ij}(1)=\bar{1}$)：

$$\bar{h} = \bar{h}_{12}(u_2)\bar{h}_{13}(u_3)\cdots\bar{h}_{1n}(u_n), \ \forall u_j \in R^\cdot$$

另一方面，Steinberg 同态 $\phi: \mathrm{St}(R) \to \mathrm{E}(R)$诱导出同态$\bar{\phi}: H/C^* \to \mathrm{E}(R)$使

$$\bar{\phi}(\bar{h}) = \mathrm{diag}(x, u_2^{-1}, \cdots, u_n^{-1}, 1\cdots)$$

(用命题 26.1(3))，其中 $x = u_n u_{n-1} \cdots u_2$，而由 C 的定义可知，当 $\bar{h} \in C/C^*$ 时，$\bar{\varphi}(\bar{h}) = \bar{1}$，即 $u_2 = u_3 = \cdots = u_n = x = 1$。因此 $\bar{h} = 1$。由此即知 $C/C^* = 1$。

□

注意 $C = W \cap K_2(R)$，由命题 26.2 立得

命题 26.3 设 $R \in \mathfrak{R}\mathrm{ing}$，则

$$K_2(R) = \langle\{\{u, v\} \mid u, v \in R^\cdot, \ uv = vu\}\rangle = C \Leftrightarrow K_2(R) \subseteq W$$

当 $R^\cdot \in \mathcal{A}G$(比如 $R \in \mathcal{C}\mathrm{Ring}$)时，

$$K_2(R) = \langle\{R^\cdot, R^\cdot\}\rangle \Leftrightarrow K_2(R) \subseteq W$$

由此命题知：研究 $K_2(R) \subseteq W$ 的条件是有重要意义的。

在§10 中，我们已定义上(下)三角初等矩阵在 ϕ 下的原象生成的 St(R)之子群

$$T = T(R) = \langle\{x_{ij}(a) \mid i < j\}\rangle,$$

$$(T' = T'(R) = \langle\{x_{ij}(a) \mid i > j\}\rangle)。$$

并证明了(见命题 10.3)$T \cap K_2(R) = T' \cap K_2(R) = 1$。即 $\phi|_T(\phi|_{T'})$为单同态。现在对除环，特别是域，我们来证明 $K_2(R) \subseteq W$。

命题 26.4 设 R 为除环，则

(1) $K_2(R) \subseteq W$，因此

$$K_2(R) = C = \langle\{\{u, v\} \mid u, v \in R^\cdot, uv = vu\}\rangle;$$

(2) $\mathrm{St}(R) = TWT$；

(3) $\forall n \geqslant 3$，$\mathrm{St}_n(R)$为 $E_n(R)$的中心扩张。

证 (1) 由命题 26.1 知 $x_{ji}(R)\subset w_{ij}(R^{\cdot})x_{ij}(R)w_{ij}(R^{\cdot})$，因此

$$\mathrm{St}(R)=\langle T,w_{ij}(R^{\cdot})\mid i<j\rangle$$

再由命题 26.1 又知

$$w_{i,i+2}(R^{\cdot})\subseteq w_{i+1,i+2}(R^{\cdot})w_{i,i+1}(R^{\cdot})w_{i+1,i+2}(R^{\cdot}),$$

$$w_{i,i+r+1}(R^{\cdot})\subseteq w_{i+r,i+r+1}(R^{\cdot})w_{i,i+r}(R^{\cdot})w_{i+r,i+r+1}(R^{\cdot})$$

从而有

$$\mathrm{St}(R)=\langle T,w_{i,i+1}(R^{\cdot})\rangle \tag{3}$$

下面来证明

$$\mathrm{St}(R)=TWT \tag{4}$$

由(3)式只需证 $w_{i,i+1}(R^{\cdot})\subset TWT$，这又归为证明

$$WTw_{i,i+1}(R^{\cdot})\subseteq TWT \tag{5}$$

因为由此可知 $TWTw_{i,i+1}(R^{\cdot})\subseteq TTWT=TWT$，而 TWT 关于取逆是封闭的，于是 $w_{i,i+1}(R^{\cdot})\subseteq TWT$。

事实上，由命题 10.3 之证知，$\forall t\in T$，t 可表如

$$t=C_n(\alpha_n)C_{n-1}(\alpha_{n-1})\cdots C_2(\alpha_2),$$

其中 $\alpha_r=(a_1,\cdots,a_{r-1})^T\in R^{r-1}$，$C_r(\alpha_r)=x_{1r}(a_1)x_{2r}(a_2)\cdots x_{r-1,r}(a_{r-1})$，而 $C_j(0)=1$，$\forall j\in N$。于是可令 $n>i+1$(设 $n\geqslant 3$)且

$$t=C_{i+1}(\alpha_{i+1})C_n(\alpha_n')\cdots C_{i+2}(\alpha_{i+2}')C_i(\alpha_i)\cdots C_2(\alpha_2)$$

由此知，必有 $a,b\in R$，$t'\in T$ 使

$$t=x_{i,i+1}(a)t',\ t'=\prod_{\substack{(k,l)\neq(i,i+1)\\ k<l}}x_{kl}(b)$$

又由命题 26.1 知，$\forall w'\in w_{i,i+1}(R^{\cdot})$，$w'^{-1}x_{kl}(b)w'\in T$。于是

$$tw'=x_{i,i+1}(a)w'(w'^{-1}t'w')\in x_{i,i+1}(R)w_{i,i+1}(R^{\cdot})T$$

因此

$$Tw_{i,i+1}(R^{\cdot})\subseteq x_{i,i+1}(R)w_{i,i+1}(R^{\cdot})T$$

从而知道(同左乘 W)，为证(5)式，只要证

$$Wx_{i,i+1}(R)w_{i,i+1}(R^{\cdot})\subseteq TWT$$

为此任取 $w\in W$。设 $\phi(w)=PD$，P 对应 σ，而 $\sigma(i)=p$，$\sigma(i+1)=q$，则

$$wx_{i,i+1}(R)w^{-1}\subseteq x_{pq}(R)$$

在 $p<q$ 时，$x_{pq}(R)\subset T$，因此

$$\begin{aligned}wx_{i,i+1}(R)w_{i,i+1}(R^{\cdot})&=(wx_{i,i+1}(R)w^{-1})ww_{i,i+1}(R^{\cdot})\\&\subseteq x_{pq}(R)ww_{i,i+1}(R^{\cdot})\subseteq TW\subseteq TWT\end{aligned}$$

在 $p>q$ 时，$\forall a\in R$(除环)，$a=0$ 或 $a\in R^{\cdot}$($a=0$ 时 $x_{i,i+1}(a)=1$)。

$a=0$ 时，$wx_{i,i+1}(0)w_{i,i+1}(R^\cdot)=ww_{i,i+1}(R^\cdot)\subseteq W\subseteq TWT$。

$a\in R^\cdot$ 时，由 $w_{ij}(u)$的定义知

$$\begin{aligned} x_{i,i+1}(a) &= w_{i,i+1}(a)x_{i,i+1}(-a)x_{i+1,i}(a^{-1}) \\ &\in w_{i,i+1}(R^\cdot)x_{i,i+1}(R)x_{i+1,i}(R^\cdot). \end{aligned}$$

于是

$$\begin{aligned} wx_{i,i+1}(a)w_{i,i+1}(R^\cdot) \subseteq ww_{i,i+1}(R^\cdot) \\ x_{i,i+1}(R)x_{i+1,i}(R^\cdot)w_{i,i+1}(R^\cdot) \end{aligned}$$

再用命题 26.1 又得

$$\begin{aligned} ww_{i,i+1}(R^\cdot)x_{i,i+1}(R) &= wx_{i+1,i}(R)w_{i,i+1}(R^\cdot) \\ &= (wx_{i+1,i}(R)w^{-1})ww_{i,i+1}(R^\cdot) \subseteq x_{qp}(R)ww_{i,i+1}(R^\cdot) \subseteq TW \\ x_{i+1,i}(R)w_{i,i+1}(R^\cdot) &= w_{i,i+1}(R^\cdot)x_{i,i+1}(R) \subseteq WT \end{aligned}$$

因此

$$wx_{i,i+1}(a)w_{i,i+1}(R^\cdot) \subseteq (TW)(WT) \subseteq TWT$$

即(5)成立，从而(4)成立。

现在来证 $K_2(R)\subseteq W$。

$\forall x\in K_2(R)$，由(4)知，必有 $t_1,t_2\in T, w\in W$ 使 $x=t_1wt_2$。于是

$$1 = \phi(x) = \phi(t_1)\phi(w)\phi(t_2)$$

由此知，$\phi(t_1^{-1}t_2^{-1})=\phi(w)$。再由命题 10.3 之证知

$$\phi(t_1^{-1}t_2^{-1}) = \begin{pmatrix} 1 & & * & \\ & \ddots & & \\ & & 1 & \\ & O & & \ddots \end{pmatrix} = PD = \phi(w)$$

因此，$\phi(t_1^{-1}t_2^{-1})=\phi(w)=1$。而由 $\phi|_T$ 单(命题 10.3)知 $t_1^{-1}t_2^{-1}=1$，即 $t_2=t_1^{-1}$。又由 $\phi(w)=1$ 知：$w\in \mathrm{Ker}\phi=C(\mathrm{St}(R))=K_2(R)$(§10)。于是

$$x = t_1wt_2 = t_1t_2w = w \in W$$

即 $K_2(R)\subseteq W$。再由命题 26.3 即知 $K_2(R)=C=\langle\{\{u,v\}\mid u,v\in R^\cdot, uv=vu\}\rangle$。

(2) 已由上面证出。再注意上面的证明对 $n\geq 3$ 均有效。从而(3)也成立。 □

将此命题用于域，立得

定理 26.1 (Matsumoto Hideya(松本英也，1939—)定理的弱形式)

设 F 为域，则

$$K_2(F) = C = \langle\{F^\cdot, F^\cdot\}\rangle$$

事实上,Matsumoto 定理的原始形式是:设 F 为域,则

$$K_2(F) = \langle \{\{F^\cdot, F^\cdot\} \mid \{u_1u_2, v\} = \{u_1, v\}\{u_2, v\}, \{u, v_1v_2\} = \{u, v_1\}\{u, v_2\}, \{u, 1-u\} = 1 (\text{其中 } u \neq 1), \ \forall u, v, u_i, v_i \in F^\cdot\}\rangle。$$

其证明可参看[Milnor,1971]。1990 年 H. Hutchinson 在《K-Theory》杂志上给出了较简单的新证明,但用到不少同调工具,有兴趣的读者可参看[Hutchinson,1990]。注意,这条定理从理论上完全解决了域的 K_2 群的确定问题(给出了生成系与关系集),而且 M. R. Stein 又将定理 26.1 推广到满足 $R=\Sigma R^\cdot$ 的交换半局部环,但即使对于域的 K_2 群,从生成系与关系集仍难以看出其具体结构(sylow 子群,有限阶子群,有限阶元的情况等)。因此这方面的工作目前仍在进行着,且是代数数论与代数 K 理论都感兴趣的热门问题之一。下面我们将简单地介绍这方面的研究动态,以作为本节的附录。在此之前,先将定理 26.1 的一个有用的推论,以及有限域 K_2 群的平凡性结果给出。

推论 26.2 若 R 为 Artin 半单环,$R=D_1^{n_1\times n_1}\oplus\cdots\oplus D_m^{n_m\times n_m}$,则

$$K_2(R) \simeq \begin{cases} \bigoplus_{j=1}^{m} \langle\{D_j^\cdot, D_j^\cdot\}\rangle, & D_j \text{ 均为域时} \\ \bigoplus_{j=1}^{m} \langle\{\{u_j, v_j\} \mid u_j, v_j \in D_j^\cdot, u_jv_j = v_ju_j\}\rangle, & D_j \text{ 均为除环时} \end{cases}$$

定理 26.2 设 $\mathbb{F}_q$ 为 q 元有限域,则 $K_2(\mathbb{F}_q)=1$ 是平凡的。

证 由命题 25.1 与定理 26.1 即得。 □

注① 可以证明,若 F 为域,则 $K_i(F[x])\simeq K_i(F)$,$i=0,1,2$。

现在简述一下数域的 K_2 群的研究动态,作为本节的附录。

附录 关于数域的 K_2 群

Ⅰ. 数域的 K_2 群

数域(有理数域 $\mathbb{Q}$ 的有限扩张)以及有限域上的一元有理函数域统称为**整体域**(global field),而**局部域**(local field)则指关于离散赋值完备且剩余类域有限的域(如 $\mathbb{R}$,$\mathbb{C}$,p-adic 数域(即 $\mathbb{Q}_p$ 的有限扩张)及有限域上的幂级数域的有限扩张)。如众周知:整体域的 K_2 群都是挠群(即一切元素都是有限阶元),因此确定 K_2 群中的有限阶元是代数 K 理论中一个重要问题。1976 年 J. Tate 在《Invent. Math., 36:25—274》中证明了:若 $\mathrm{Ch}F \nmid n$ 且整体域 F 含 n 次本原单位根 ξ_n,则 K_2F 中任一 n 阶元素都可表如 $\{\xi_n, a\}$,其

中 $a\in F^{\cdot}$(为方便起见下面都将 $K_2(R)$ 简记为 K_2R)。1987 年 A. A. Suslin 在《K－Theory ,1:5－29》上将此结果推广到含 ξ_n 的任意域上。对 K_2F 中的小阶元,J. Browkin 于 1982 年在《LNM. 966.1－6》中证明了如下结果:

(1) 若 $\xi_n\in F\neq \mathbb{F}_2$ 且 $n=1,2,3,4,6$ 时,K_2F 中的每一个元素 $\{\xi_n,y\}$ 都可表如 $\{a,\Phi_n(a)\}$,其中 $a,\Phi_n(a),y\in F^{\cdot}$,$\Phi_n(x)$ 为第 n 个分圆多项式;

(2) 记 $G_n=\{\{a,\Phi_n(a)\}\mid a,\Phi_n(a)\in F^{\cdot}\}$,则 $\forall\alpha\in G_n,\alpha^n=1$ 且在 $F\neq \mathbb{F}_2$,$n=1,2,3,4,6$ 时 G_n 为 K_2F 的子群;

(3) $K_2\mathbb{Q}$ 的 3 阶元都可表如 $\{a,a^2+a+1\}$,即 $\{a,\Phi_3(a)\}$,$a\in\mathbb{Q}^{\cdot}$,因此 $(K_2\mathbb{Q})_3=G_3(\mathbb{Q})$,其中 $(K_2F)_p$ 表 K_2F 的 p-sylow 子群。因此,此时 $(K_2\mathbb{Q})_3$ 为 3 阶循环群;

(4) $K_2\mathbb{Q}$ 的 4 阶元都可表如 $\{a,a^2+1\}v$,即 $\{a,\Phi_4(a)\}v$,其中 $a\in\mathbb{Q}^{\cdot}$,$v\in K_2\mathbb{Q}$ 且 $v^2=1$。

Browkin 据此猜想:

(A) 对任意域 F 与 $n\neq 1,2,3,4,6$,(1),(2)都不成立,特别地,$G_5(\mathbb{Q})$ 不是群;

(B) (3),(4)对一切域都成立。

1988 年,J. Urbanowicz 在《J. Pure and Appl. Alg., 50:295－307》中证明了(3)对一切特征数非 3 的域都成立;1993 年秦厚荣在《科学通报,1993.12》中证明了(4)对一切特征数非 2 的域都成立,且 $F=\mathbb{Q}$ 时,G_{2^n} 为群 $\Leftrightarrow n=1,2$,同时他证出 $G_5(\mathbb{Q})$,$G_7(\mathbb{Q})$ 都不是群。因此(B)已接近解决(仅余下 $\mathrm{Ch}F=2,3$ 的情况)。2001 年徐克舰与秦厚荣在《中国科学(A 辑),31:11—17》中证明了猜想 A 对局部域一般地并不成立,而且使(1),(2)成立的情况比 Browkin 猜想的要大得多,从而比猜测(A)成立更能显示研究群 G_n 的意义。对整体域,徐克舰 2001 年在南京大学的博士论文中又进一步证明了:若 $n\geqslant 2$,则 $G_{2^n3^m}(\mathbb{Q})$ 为 $K_2\mathbb{Q}$ 之子群 $\Leftrightarrow n=2,m=0$。同时,对 $G_{p^n}(\mathbb{Q})$,证明了 $G_9(\mathbb{Q})$,$G_{11}(\mathbb{Q})$,$G_{25}(\mathbb{Q})$,$G_{49}(\mathbb{Q})$,$G_{27}(\mathbb{Q})$ 都不是群。对 $\mathbb{Q}(i)$ 与 $\mathbb{Q}(\sqrt{-2})$,证明了:$G_{2^n}(\mathbb{Q}(i))$ $(G_{2^n}(\mathbb{Q}(\sqrt{-2})))$ 是群 $\Leftrightarrow n\leqslant 2$,且 $n\geqslant 2$ 时,$G_{2^n3^m}(\mathbb{Q}(\sqrt{-2}))$ 是群 $\Leftrightarrow n=2,m=0$。从而又部分地证实了猜想(A)。

Ⅱ. Birch-Tate 猜想:

设 F 为全实的数域(即 $F<\mathbb{R}$),$W_2(F)$ 为 $F(\sqrt{F})$ 中单位根的个数,而

$$\zeta_F(s)=\sum_{0\neq A\lhd O_F}N(A)^{-s}=\prod_{0\neq P\in \mathrm{Spec}O_F}1/(1-(N(p))^{-s}),\ s\in\mathbb{C}$$

为 F 上的 Dedekind ζ-函数(当 $\mathrm{Re}s>1$ 时绝对收敛),则

$$|K_2O_F|=W_2(F)\,|\zeta_F(-1)| \qquad (*)$$

1984 年 B. Mazur 与 A. Wiles 在《Invent. Math., 76:179—330》中证出：当 F 为全实的 Abel 数域(指 $F/\mathbb{Q}$ 的 Galois 群为 Abel 群)时，(*)两端的奇数部分相等。1986 年 M. Kolster 在《Comment. Math. Helv., 61:376—388》中基于上述结果又证明了：若 K_2O_F 的 2-sylow 子群为初等 Abel 群(一个 Abel 群 G 称为初等的，是指有素数 p 使对 $\forall g\in G, g^p=1$)时(*)成立。1990 年 A. Wiles 在《Ann. Math., 131:493—540》中指出：在全实 Abel 数域情况下(*)已完全证出。注意循环扩张(即 Galois 群为循环群的扩张)必为 Abel 扩张。特别地，在实二次域(Galois 群为 2 阶循环群)的情况下，(*)，即 Birch-Tate 猜测，是成立的。

Ⅲ. 二次域整元环的 K_2 群

虚二次域整元环的 K_2 群的一些研究情况已在上节末作了简单介绍。实二次域 F 的整元环 O_F 的 K_2 群更为复杂，对 K_2O_F 的 2-sylow 子群 $(K_2O_F)_2$ 的研究在 1993 年之前也只限于初等 Abel 群的情况。1993 年秦厚荣在《中国科学(A 辑), 23:1254—1263》中突破了这个限制，给出了研究 $(K_2O_F)_2$ 的更一般的方法，他的方法只需计算一些 Legendre 符号，即可确定 2-sylow 子群的结构。他证明了：若 $F=\mathbb{Q}(\sqrt{d})$ 为实二次域，$d=p_1p_2p_3$(三素数之积)，在 12 种情况下(如 $(p_1,p_2,p_3)\in(1,3,7)\bmod 8$，$\left(\frac{p_2}{p_1}\right)=\left(\frac{p_3}{p_1}\right)=-1$ 即其中的一种情况)，$(K_2O_F)_2\simeq\mathbb{Z}_2\oplus\mathbb{Z}_2\oplus\mathbb{Z}_4$(非初等 Abel 群！)且除在情况(10)外，$(\mathscr{R}_2F)_2\simeq\mathbb{Z}_2\oplus\mathbb{Z}_2$，情况(10)下 $(\mathscr{R}_2F)_2\simeq\mathbb{Z}_2$，其中 $\mathscr{R}_2F$ 表示 F 的**野(wild)核**。事实上，D. Quillen 与 C. Moore 对任意数域给出了正合列(第一个正合列与上节末所述的正合列是一致的)：

$$0\to \underset{(\text{驯核})}{K_2O_F}\to K_2F\xrightarrow{\tau}\coprod_{p\text{为有限位}}\bar{F}_p^*\to 0$$

$$0\to \underset{(\text{野核})}{\mathscr{R}_2F}\to K_2F\xrightarrow{\eta}\coprod_{p\text{非复位}}\mu_p\to\mu\to 0$$

其中的位 p 指环同态 $p:F\to K(\text{域})\cup\{\infty\}$，此同态核的元素集为环 $p^{-1}(K)$ 的素理想——对应 p 的素除子 p。$\bar{F}_p$ 为素除子 p 处的剩余类域，F_p 为 F 在 p 的完备化，

$$\tau_p\{x,y\}=(-1)^{v_p(x)v_p(y)}x^{v_p(y)}y^{-v_p(x)}\pmod{p}$$

给出 F 上对应 p 的离散赋值，μ_p 为 F_p 中的单位根群，μ 为 F 中的单位根群。η 为 Hilbert 符号诱导的同态，而 F_p 上的 Hilbert 符号 $\left(\frac{\ ,\ }{p}\right)_2$ 定义为：

$$\left(\frac{a,b}{p}\right)_2=1\Leftrightarrow \text{有 } x,y\in F_p \text{ 使 } ax^2+by^2=1,$$

$$\left(\frac{a,b}{p}\right)_2=-1 \Leftrightarrow \text{无 } x,y\in F_p \text{ 使 } ax^2+by^2=1。$$

这些将在下节中作更进一步的介绍。

对虚二次域 $F=\mathbb{Q}(\sqrt{d})$，$d<0$ 无平方因子。可将已知的类数(O_F 的类数)及 K_2O_F 列如下表：

d	-1	-2	-3	-5	-6	-7	-11	-15	-19	-35	-43
h	1	1	1	2	2	1	1	2	1	2	1
K_2O_F	1	1	1	1	1	$\mathbb{Z}_2$	1	$\mathbb{Z}_2$	1	$\mathbb{Z}_2$	1

由于 $h=1$ 的全体 d 值为：$-1,-2,-3,-7,-11,-19,-43,-67,-163$。容易由此猜测：对虚二次域 F，$h=1$ 时 $K_2O_F\simeq 1$ 或 $\mathbb{Z}_2$。这只要算出 $d=-67,-163$ 时的 K_2O_F 即可证出或推翻此猜测。再注意 $h=2$ 的全体 d 值为：$-5,-6,-10,-13,-15,-22,-35,-37,-51,-58,-91,-115,-123,-187,-235,-267,-403,-427$。算出对应的有限个 K_2O_F 也可作另一个猜测：对虚二次域 F，$h=2$ 时 $K_2O_F=1$ 或 $\mathbb{Z}_2$，注意，不能猜测对一切虚二次域 F，$K_2O_F\simeq 1$ 或 $\mathbb{Z}_2$。因为 2001 年岳勤在《数学研究与评论，21：1—6》中已算出 $d=-21$ 时(此时 $h=4$)，K_2O_F 有 6 阶元 $\{4,\sqrt{-21}-2\}$，值得注意的是他在该文中还对实二次域，证明了 $d=6$(对应的 $h=1$)时，K_2O_F 有 3 阶元 $\{6,-8+3\sqrt{6}\}$；$d=15$(对应的 $h=2$)时，$K_2O_F\simeq\mathbb{Z}_2\oplus\mathbb{Z}_8\oplus\mathbb{Z}_3$，且 $\{-1,-1\}$ 为 $\mathbb{Z}_2$ 的生成元，$\{-3,3+\sqrt{15}\}$ 为 $\mathbb{Z}_8\oplus\mathbb{Z}_3$ 的生成元；$d=29$(对应的 $h=1$)时 $K_2O_F\simeq\mathbb{Z}_2\oplus\mathbb{Z}_2\oplus\mathbb{Z}_3$，三个直和项分别有生成元 $\{-1,-1\}$，$\{-1,(5+\sqrt{29})/2\}$，$\{(1+\sqrt{29})/2,8\}$ 且野核 $\mathcal{R}_2F\simeq\mathbb{Z}_3$。值得注意的是，1982 年 J. Browkin 在《Universal Algebra and Application, Banach Center Publications, 9:187—195》中的结果：对任意数域 F，

$$|K_2O_F/\mathcal{R}_2F|=\begin{cases}3\cdot 2^i, & d\equiv -3 \bmod 9, d\neq -3\\ 2^j, & \text{其他情况}\end{cases}$$

§27　赋值与 $K_2\mathbb{Q}$

在上节中已证：任何 q 元有限域 $\mathbb{F}_q$ 的 K_2 群都是平凡的。因此有限域的 K_2 群已无研究的必要。但对一般的域 F，尽管已经知道 K_2F 由 $\{F^\cdot,F^\cdot\}$ 生成且关系集为 $\{,\}$ 的双乘性及 $\{u,1-u\}=1$，$\forall 1\neq u\in F^\cdot$，但欲知

K_2F 的具体结构仍是十分艰难的事。本节中对有理数域$\mathbb{Q}$,我们将给出 $K_2\mathbb{Q}$ 的优美的结构定理,所用的主要工具是赋值。由于用赋值可得各种各样的互反律(见下节),其重要性并不在 K_2 群之下,且赋值还可给出各种各样的满足双乘性及$(u,1-u)=1$ 的符号$(,)$(我们也称这些为 Steinberg 符号),从而又与 K_2 群有着紧密的联系,因此我们先介绍一下有关赋值的一些知识。事实上,赋值是通常实(复)数绝对值概念的推广,在代数数几何,代数数论及分析学中也都有重要的应用。

设 p 为一素数,$0\neq a\in\mathbb{Q}$,则必有 $v(a)\in\mathbb{Z}$ 使

$$a = p^{v(a)}\frac{m}{n},\ (m,p) = (n,p) = 1$$

取 ρ 使 $0<\rho<1$,令

$$\begin{aligned}\varphi:&\mathbb{Q}\to\mathbb{R},\\ &a\mapsto\rho^{v(a)},\ \forall 0\neq a\in\mathbb{Q}\\ &0\mapsto 0,\end{aligned}$$

则

(1) $\varphi(a)\geqslant 0,\forall a\in\mathbb{Q}$,且 $\varphi(a)=0\Leftrightarrow a=0$(非负性);

(2) $\varphi(ab)=\varphi(a)\varphi(b),\forall a,b\in\mathbb{Q}$(乘性);

(3) $\varphi(a+b)\leqslant\max(\varphi(a),\varphi(b)),\forall a,b\in\mathbb{Q}$(强三角不等式)。

因此 φ 为$\mathbb{Q}$ 上的非 Archimedes 赋值(绝对值,一阶赋值),称为 **p-*adic* 赋值**(p-adic valuation))。更一般地,任意域 F 到$\mathbb{R}$ 的映射 φ,若满足上述的(1),(2),(3),则称 φ 为 F 上的**非 Archimedes 赋值**。将(3)改为

(3)′ $\varphi(a+b)\leqslant C\max(\varphi(a),\varphi(b)),0<C\leqslant 2$

则称满足(1),(2),(3)′但不满足(3)的 φ 为 **Archimedes 赋值**(有时也将(3)改为

(3)″ $\varphi(a+b)\leqslant\varphi(a)+\varphi(b)$(三角不等式)

而将满足(1),(2),(3)″但不满足(3)的 φ 称为 Archimedes 赋值)。

显然对前述的 $v:\mathbb{Q}\to\mathbb{Z}$,规定 $v(0)=\infty$,则得映射

$$v\equiv v_p:\mathbb{Q}\to\mathbb{Z}\cup\{\infty\}$$

且满足

$$\begin{aligned}&v(ab) = v(a)+v(b),\ \forall a,b\in\mathbb{Q};\\ &v(a+b)\geqslant\min\{v(a),v(b)\},\ \forall a,b\in\mathbb{Q};\\ &v(0)=\infty。\end{aligned}$$

称 $v=v_p$ 为$\mathbb{Q}$ 上对应于 p 的**指数赋值**(exponential valuation)。

由此可给出如下定义

定义 27.1　设 p 为素数，$p\neq 2$ 时，定义

$$d_v(x,y)=(-1)^{v(x)v(y)}x^{v(y)}/y^{v(x)}\ (\mathrm{mod}\ p)$$

则

$$d_v\equiv d_{v_p}:\mathbb{Q}^\cdot\times\mathbb{Q}^\cdot\rightarrow\mathbb{Z}_p^\cdot\equiv A_p(p-1\text{ 阶循环群})$$

称为 $\mathbb{Q}$ 上关于 v_p 的**驯符号**（tame symbol），记为

$$(x,y)_p\equiv d_{v_p}(x,y),\ \forall x,y\in\mathbb{Q}^\cdot$$

$p=2$ 时（上定义平凡，因为 $1\equiv-1\mathrm{mod}\ 2$ 且 $\mathbb{Z}_2^\cdot=1$），注意 $2\nmid a, a\in\mathbb{Z}$ 时 $a\equiv 1,3,5,7(\mathrm{mod}\ 8)\equiv\pm1,\pm3(\mathrm{mod}\ 8)$，因此 $\forall\, 0\neq x\in\mathbb{Q}$，$x$ 可惟一表为

$$x=(-1)^i2^j5^k\frac{m}{n},\quad\text{其中 } m,n\equiv 1(\mathrm{mod}\ 8)$$

比如，

$$-\frac{6}{55}=(-1)^1 2^1\cdot 5^{-1}\cdot\frac{3}{11}$$

$$=(-1)^1 2^1 5^{-1}\frac{9}{33},\ 9,33\equiv 1(\mathrm{mod}\ 8)$$

设 $0\neq y\in\mathbb{Q}$ 的这种表示为

$$y=(-1)^I2^J5^K\frac{m'}{n'},\ m',n'\equiv 1(\mathrm{mod}\ 8)$$

可定义

$$(x,y)_2=(-1)^{iI+jK+kJ}$$

则

$$(\ ,\ )_2:\mathbb{Q}^\cdot\times\mathbb{Q}^\cdot\rightarrow A_2\equiv\{\pm1\}$$

与上面的 $(\ ,\ )_p$ 都是 Steinberg 符号（满足双乘性与 $(u,1-u)=1$ 的符号 $(\ ,\ )$ 都称为 Steinberg 符号）。

另一种常用的赋值是**离散赋值**（discrete valuation）。域 F 上的离散赋值 v，是指一个群的满同态（其中的 $\mathbb{Z}$ 也可以是一个无限循环群，当然对标准序为序群）

$$v:\quad F^\cdot\ \longrightarrow\!\!\!\!\rightarrow\ \mathbb{Z}$$

（乘法群）（加法群）

且它满足

$$v(x+y)\geqslant\min\{v(x),v(y)\}\quad(\forall x,y\in F^\cdot\text{ 且}$$

$$x+y\in F^\cdot\ (\text{即 }0\neq x,y\in F, x+y\neq 0))\qquad(*)$$

记

$$\Lambda\equiv\{x\mid v(x)\geqslant 0\}\cup\{0\}\subseteq F$$

则 Λ 为交换环，称为 v 的**相伴赋值环**(associated valuation ring)。这是一个局部环，其惟一极大理想为

$$P \equiv \{x \mid v(x) > 0\} \cup \{0\},$$

称为 v 对应的**极大理想**。而 Λ/P 常记为 $\bar{F}$，称为 v 的**剩余类域**(residue class field)。

定义 27.1′ 设 F 为域，v 为 F 上的离散赋值。定义

$$d_v(x,y) = (-1)^{v(x)v(y)} x^{v(y)}/y^{v(x)} (\mathrm{mod} P), \ \forall x,y \in F^{\cdot}$$

现在来证明

命题 27.1 定义 27.1′中给出的 $d_v: F^{\cdot} \times F^{\cdot} \to \bar{F}^{\cdot} = (\Lambda/P)^{\cdot}$ 对 v 拓扑(对 v 给出的 $F^{\cdot}$ 之球形邻域诱导的 $F^{\cdot} \times F^{\cdot}$ 拓扑与 $\mathbb{Z}$ 的离散拓扑)为连续的 Steinberg 符号，且 d_v 诱导一个群的满同态：

$$\mathrm{K}_2 F \twoheadrightarrow \mathrm{K}_1 \bar{F} = \bar{F}^{\cdot}$$

证 先证 $\mathrm{Im}(d_v) \subseteq \bar{F}^{\cdot}$，为此只需证 $\pm x^{v(y)}/y^{v(x)} \in \Lambda^{\cdot}$，$\forall x, y \in F^{\cdot}$。事实上，由 v 为群同态知，

$$v(x^{v(y)}/y^{v(x)}) = v(x)v(y) - v(x)v(y) = 0$$

因此 $x^{v(y)}/y^{v(x)} \in \Lambda \backslash P$。但 Λ 为局部环，于是 $x^{v(y)}/y^{v(x)} \in \Lambda^{\cdot}$，即 $\pm x^{v(y)}/y^{v(x)} \in \Lambda^{\cdot}$。

其次，d_v 的双乘性与对 v-拓扑的连续性可直接验证。

再证 $d_v(1-x,x)=1$(即 $d_v(x,1-x)=1$)，$\forall 1 \neq x \in F^{\cdot}$，分五种情况进行验证。

(1) $v(x)>0$，此时 $x \in P$，因此 $1-x \in \Lambda$ 且 $1-x \equiv 1(\mathrm{mod}\ P)$。但由 v 为群同态及(*)式又知

$$0 = v(1) = v(1-x+x) \geqslant \min\{v(1-x), v(x)\}$$

于是 $v(1-x) \leqslant 0$。又由 $1-x \in \Lambda$ 知 $v(1-x) \geqslant 0$(注意 $1-x \neq 0$)，故 $v(1-x)=0$。因此

$$\begin{aligned} d_v(1-x,x) &= (-1)^{v(x)v(1-x)}(1-x)^{v(x)}/x^{v(1-x)} \\ &= (1-x)^{v(x)} \equiv 1(\mathrm{mod}\ P) = 1 \end{aligned}$$

(2) $v(1-x)>0$ 时与(1)同理可证。

(3) $v(x)<0$，此时 $x^{-1} \in P$，于是

$$(1-x)/x = -1 + x^{-1} \equiv -1(\mathrm{mod}\ P)$$

从而由 Λ 为局部环知 $(1-x)/x \in \Lambda^{\cdot} = \Lambda \backslash P$。因此 $v((1-x)/x)=0$，于是 $v(1-x)=v(x)$(v 为群同态!)。由此可得

$$d_v(1-x,x) = (-1)^{v(1-x)v(x)}(1-x)^{v(x)}/x^{v(1-x)}$$

$$= (-1)^{v(x)}((1-x)/x)^{v(x)}$$

$$\equiv (-1)^{v(x)}(-1)^{v(x)} \equiv 1(\mathrm{mod}\ P) = 1$$

(4) $v(1-x)<0$ 时与(3)同理可证。

(5) $v(x)=v(1-x)=0$ 时显然。

这就证出了 $d_v(1-x,x)=1, \forall 1\neq x\in F^{\cdot}$。

最后,注意 Matsumoto 定理(原始形式,见定理 26.1 下一段)指出$\{,\}$的关系集是任意 Steinberg 符号关系集的子集,这意味着$\{,\}$为**泛 Steinberg 符号**,即对任意的 Abel 群 G,任意的 Steinberg 符号 C: $F^{\cdot}\times F^{\cdot}\to G$,必有惟一的群同态 f: $K_2(F)\to G$ 使 $f\{,\}=c$,因此取 $C=d_v$ 知,d_v 诱导一个群同态 $K_2F\to K_1\bar{F}=\bar{F}^{\cdot}$。再由 v 为满同态知必有 $y\in F^{\cdot}$ 使 $v(y)=1$,由此知 d_v 是满的。因此 d_v 诱导的上述群同态也是满的。 □

为介绍上述命题的应用,需更深刻地认识赋值(注意$\mathbb{R}(\mathbb{C})$中绝对值的定义及性质只用到其乘法结构与序结构)。为此在更一般的情况下,给出下述定义(建议读者将下定义中 Γ 的运算改用加法,添加 0 于 Γ 改为添加∞,修改(2),(3),(4),给出**加法赋值(Krull 赋值)**的定义)。

定义 A　设 F 为域,Γ 为序群(乘法运算),φ:$F\to\Gamma\cup\{0\}$(在$\Gamma\cup\{0\}$中,$0\cdot\lambda=\lambda\cdot 0=0\cdot 0=0, 0<\lambda, \forall\lambda\in\Gamma$)满足

(1) φ 为满射;

(2) $\varphi(a)=0\Leftrightarrow a=0_F$;

(3) $\varphi(ab)=\varphi(a)\varphi(b)$, $\forall a,b\in F$;

(4) $\varphi(a+b)\leqslant\max\{\varphi(a),\varphi(b)\}, \forall a,b\in F$,

则称 φ 为 F 上的一个**赋值**,Γ 称为 φ 的**值群**(value group)(又称(F,φ)为**赋值域**(valuation field))。在 $\varphi(F)=1$ 时,称 φ 为 F 上的**平凡赋值**(trivial valuation),也称为**浅显赋值**。

注意 $\Gamma\neq 1$ 时必有$|\Gamma|=\infty$(因为 $\lambda\in\Gamma,\lambda<1$ 时,$\lambda^k<1,\forall k>0$,于是 $\mathrm{ord}\lambda=\infty$)。因此$|F|<\infty$时(由于 φ 满,必有 $\varphi(F^{\cdot})=1$),即有

命题 27.2　有限域上的赋值(包括离散赋值)都是平凡的。

记 $B_\varphi=\{a\in F|\varphi(a)\leqslant 1\}, M_\varphi=\{a\in F|\varphi(a)<1\}$,则 B_φ 为交换的局部环,M_φ 为其惟一的极大理想,称 B_φ 为 φ 的**赋值(整)环**(显然,$a,b\in B_\varphi$ 时必 $a|b$ 或 $b|a$),M_φ 为 φ 的**极大理想**,并称 $\bar{F}_\varphi\cong B_\varphi/M_\varphi$ 为 φ 的**剩余类域**。

当 $\Gamma\simeq\mathbb{Z}$,即 φ 为离散赋值时,又称 B_φ 为**离散赋值(整)环**(DVR, discrete valuation ring)。显然,对离散赋值环 B_φ,$B_\varphi\in$ PID 且 B_φ 恰有一个非零素理想。

在环论中(脱离赋值)可更一般地定义赋值环与离散赋值环的概念。

即,设 R 为整环,且 $\forall a,b\in R, a|b$ 或 $b|a$,则称 R 为**赋值环**;设 $R\in$ PID 且 R 有惟一的非零素理想,则称 R 为**离散赋值环**(DVR)。不难证明:① 设 R 为赋值环,则 $R\in$ DVR$\Leftrightarrow R\in$ PID$\Leftrightarrow R$ 为 Noether 环;② $R\in$ DVR$\Leftrightarrow R$ 为 Noether 整闭整环且有惟一非零素理想$\Leftrightarrow R\in$ PID 且为局部环但非域;③ R 为赋值环$\Leftrightarrow R$ 为整环,且 $\forall x\in Q(R)$(R 的分式域),$x\in R$ 或 $x^{-1}\in R$;④ DVR 为赋值环;⑤ R 为 Prüfer 环(即一切有限生成理想均可逆的整环)$\Leftrightarrow$ $\forall P\in \mathrm{Spec}R, R_P$ 为赋值环;⑥ R 为 Dedekind 环$\Leftrightarrow$ R 为 Noether 环且 $\forall P\in \mathrm{Spec}R, R_P$ 为离散赋值环(定理 22.1);⑦ 赋值环都是局部环。

下面我们来说明:赋值环,赋值以及位,三者实质上是一一对应的,为此先介绍位的定义。

定义 B 设 F,K 为域,映射 $\pi: F\to K\cup\{\infty\}$满足

(1) $B=\{a\in F|\pi(a)\in K\}$为 F 的子环;

(2) $\pi|_B: B\to K$ 为环同态;

(3) $\pi(a)=\infty$时 $\pi(a^{-1})=0$,其中 $a\in F$,

则称 π 为 F 的一个**K-位**(K-place,俄语为 K-точка,是"点"的意思)。$\pi|_B$ 为单同态时 $B=F$,此时又称 π 为 F 的一个**浅显位**(trivial place)。

说明位的一个佳例是下例(在例中位 π 事实即复平面的点)。

例 1 设 $F=\mathbb{C}(x)$(复系数一元有理函数域),$\forall \alpha\in\mathbb{C}$,令 $x\mapsto\alpha$,注意任意的 $f(x)/g(x)\in F,(f(x),g(x))=1$。若 $g(\alpha)\neq 0$,则定义 $f(x)/g(x)\mapsto f(\alpha)/g(\alpha)$,$g(\alpha)=0$ 时规定 $f(x)/g(x)\mapsto\infty$,则得 $\pi: \mathbb{C}(x)\to\mathbb{C}\cup\{\infty\}$。$\pi$ 为 $F=\mathbb{C}(x)$的一个$\mathbb{C}$-位。$\pi(f(x)/g(x))=0$ 时称 $f(x)/g(x)$在 α 处有零点(有零点 α);$\pi(f(x)/g(x))=\infty$时称 $f(x)/g(x)$在 α 处有极点(有极点 α)。记

$$B=\{f(x)/g(x)\in F\mid g(\alpha)\neq 0\},$$
$$U_B=\{f(x)/g(x)\in F\mid f(\alpha)\neq 0,\ g(\alpha)\neq 0\}$$

注意 $f(x)/g(x)$总可表为$(x-\alpha)^n a(x)/b(x)$,其中 $n\in\mathbb{Z}$,$a(x)/b(x)\in U_B$。且任意 ρ 使 $0<\rho<1$,B 给出赋值 $\varphi: F=\mathbb{C}(x)\to\mathbb{R}$ 使

$$\varphi((x-\alpha)^n a(x)/b(x))=\rho^n$$

这也是一种 p-adic 赋值,且是离散赋值,它可指出零点、极点的阶数。

更一般地,可以看出定义 B 中的 B 为**赋值环**,常记 B 为 B_π,称为位 π 的**赋值环**,其惟一的极大理想为

$$M_\pi=\{a\in B\mid a^{-1}\notin B\}=\{a\mid \pi(a)=0\}$$

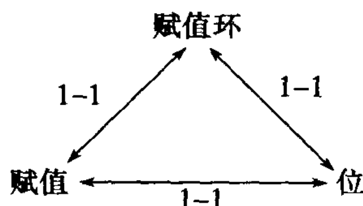
称为位 π 的**极大理想**,而 $\bar{F}=B_\pi/M_\pi$ 称为位 π 的**剩余类域**。反过来,若 B 为域 F 中的一个赋值环,记其惟一极大理想为 M,则有标准环同态

$$\pi_B: B \twoheadrightarrow B/M = \bar{F}$$

规定 $\pi_B(F\backslash B)=\infty$，则 π_B 为 F 的一个位，称为 F 的**正规位(标准位)**(normal place)。对 F 的两个位：$\pi_i:F\to K_i\cup\{\infty\}$，$i=1,2$，若有域同构 $\theta:K_1\to K_2$ 使 $\theta\pi_1=\pi_2$，则称位 π_1 与 π_2 等价，记为 $\pi_1\sim\pi_2$。可以证明 $\pi_1\sim\pi_2\Leftrightarrow B_{\pi_1}=B_{\pi_2}$。因此赋值环与位是互相确定的，且在等价意义下是一一对应的。对域 F 上的赋值 $\varphi_i:F\to\Gamma_i\cup\{0\}$，$i=1,2$，若有序群同构 $\theta:\Gamma_1\to\Gamma_2$ 使 $\theta\varphi_1=\varphi_2$，则也称赋值 φ_1,φ_2 是等价的，记为 $\varphi_1\sim\varphi_2$，也可证明 $\varphi_1\sim\varphi_2\Leftrightarrow B_{\varphi_1}=B_{\varphi_2}$。由域 F 内的任意赋值 B 也可给出一个赋值，即令 M 为 B 的惟一极大理想，记 $U_B=B\backslash M$，则 $U_B=B^{\cdot}\lhd F^{\cdot}$，令 $\Gamma=F^{\cdot}/U_B$，$M^*=M\backslash\{0\}$，$M^{*^{-1}}=\{a^{-1}\mid a\in M^*\}$，则显见 $F=M\cup U_B\cup M^{*^{-1}}$。再记 $\Delta=\{aU_B\mid a\in M^*\}=M^*U_B$，则 Δ 满足：① $1=1_\Gamma\notin\Delta$；② $\forall\, 1\neq\lambda\in\Gamma$，$\lambda\in\Delta$ 或 $\lambda^{-1}\in\Delta$，但$\{\lambda,\lambda^{-1}\}\not\subset\Delta$；③ $\lambda,\mu\in\Delta$ 则 $\lambda\mu\in\Delta$，即 Γ 为一个序群(序由 Δ 给出：规定 $\lambda\leqslant\mu$ 当且仅当 $\lambda\mu^{-1}\in\Delta\cup\{1\}$)。于是 $aU_B\leqslant 1\Leftrightarrow a\in B$。令 $\varphi_B:F\to\Gamma\cup\{0\}$

$$\varphi_B(a)=\begin{cases}aU_B, & 0\neq a\in F\\ 0, & 0=a\in F\end{cases}$$

则 φ_B 为 F 上由 B 确定的赋值。由此知，对一个域 F，在等价意义下有下述的一一对应：



定义 C　设(F,φ)，(K,ψ)为两个赋值域。若 $F<K$(代数扩张或超越扩张)且 $\varphi=\psi|_F$，则记$(F,\varphi)\leqslant(K,\psi)$且称$(K,\psi)$为$(F,\psi)$的**扩张**(extension)(可证：$(F,\varphi)\leqslant(K,\psi)\Leftrightarrow B_\psi\cap F=B_\varphi$)。

若又 $\varphi:F\to\Gamma\cup\{0\}$，$\psi:K\to\Lambda\cup\{0\}$，则 $\Gamma\lhd\Lambda$ 且 $\bar{F}_\varphi<\bar{K}_\psi$，称 $e(\psi|_F)\equiv(\Lambda:\Gamma)=|\Lambda/\Gamma|$为 ψ 在 F 上的**分歧指数**(ramification index)。若 $\bar{K}_\psi>\bar{F}_\varphi$ 为代数扩张，则称 $f(\psi|_F)\equiv[\bar{K}_\psi:\bar{F}_\varphi]$为 ψ 在 F 上的**剩余次数**(residue degree)。

在 $e(\psi|_F)=1$ 时，称(K,ψ)为(F,φ)的**非分歧扩张**(nonramified extension)，在 $e(\psi|_F)=f(\psi|_F)=1$ 时称(K,ψ)为(F,φ)的**直接扩张**(directed extension)。可以证明：当$[K:F]<\infty$时，$e(\psi|_F)$，$f(\psi|_F)\leqslant[K:F]$。

下面来证明关于域的 K_2 群阶数的一个结果：

定理 27.1　对任意域 F，$|F|>\aleph_0\Leftrightarrow|K_2F|>\aleph_0$。

证 $\Rightarrow$:令 Π 为 F 的素子域(最小子域),$X=\{x_a\mid a\in A\}$ 为 F 在 Π 上的极大代数无关元的集合,则 $F>\Pi(X)$ 为代数扩张。由于 $|F|>\aleph_0$ 可知 $|\Pi(X)|>\aleph_0$。取 $x_0\in X$,$X'=X\setminus\{x_0\}$,则有一个位 $\pi:\Pi(X)\to\Pi(X')$ 使 $f(x_0)\mapsto f(0)$。仿例 1 知必有 $\Pi(X)$上的离散赋值使其剩余类域为$\Pi(X')$,将 π 开拓为 F 的位(一个域的位总可开拓到其扩张(代数或超越扩张)域上的位(仍记为 π))$\pi:F\to\Pi(X')$的代数闭包,于是对任意的满足 $\Pi(X)<E<F$ 与$[E:\Pi(X)]<\infty$的 E,必有 E 上的离散赋值,使其剩余类域 $\bar{E}\underset{\text{f. g.}}{>}\Pi(X')$。因此由命题 27.1 知,有满同态 $K_2E\twoheadrightarrow\bar{E}^{\cdot}$。

令 $E_1>E$ 有分歧指数 r,则有交换图

$$\begin{array}{ccc} K_2E & \longrightarrow & K_2E_1 \\ \downarrow & & \downarrow \\ \bar{E} & \xrightarrow[e\mapsto e^r]{r} & \bar{E} \end{array}$$

模去单位根群〈{单位根}〉(可数阶子群)得交换图

$$\begin{array}{ccc} K_2E & \longrightarrow & K_2E_1 \\ \downarrow & & \downarrow \\ \bar{E}/\langle\{\text{单位根}\}\rangle & \rightarrowtail & \bar{E}_1/\langle\{\text{单位根}\}\rangle \end{array}$$

用 K_2 群对正向极限的连续性(见 § 13)得满同态

$$\varinjlim_{\substack{\Pi(X)<E<F\\ [E:\Pi(X)]<\infty}}{}' K_2E=K_2F\twoheadrightarrow\varinjlim_{\substack{\Pi(X)<E<F\\ [E:\Pi(X)]<\infty}}\bar{E}^{\cdot}/\langle\{\text{单位根}\}\rangle$$

因此,由 $|\Pi(X)|>\aleph_0$ 知 $|K_2F|>\aleph_0$。

$\Leftarrow$: 注意 $K_2F=\langle\{F^{\cdot},F^{\cdot}\}\rangle$,若 $|F|\leqslant\aleph_0$,则 $|K_2F|\leqslant\aleph_0$,即得证。□

下面再来证明前述的$(\,,)_p$ 为泛连续 Steinberg 符号。

命题 27.2 设 p 为素数,A 为 Hausdorff 拓扑群,$c:\mathbb{Q}_p^{\cdot}\times\mathbb{Q}_p^{\cdot}\to A$ 为(关于$\mathbb{Q}_p^{\cdot}$ 的 p-adic 拓扑)连续的 Steinberg 符号,则必有惟一的拓扑群同态 $h:A_p\to A$(其中 $A_p=\mathbb{Z}_p^{\cdot}$ ($p\neq2$ 时)或$\{\pm1\}$($p=2$ 时)),使

$$h((x,y)_p)=c(x,y),\qquad\forall x,y\in\mathbb{Q}_p^{\cdot}$$

即有下述的交换图

$$\begin{array}{ccc} \mathbb{Q}_p^{\cdot}\times\mathbb{Q}_p^{\cdot} & \xrightarrow{c} & A \\ {\scriptstyle(,)_p}\downarrow & \nearrow_{\exists 1\, h} & \\ A_p & & \end{array}$$

因此，$(\ ,\ )_p$ 为$\mathbb{Q}$上的泛连续 steinberg 符号。

证 令 $p^n>2$，由二项式定理即得

$$(1-rp^n)^p \equiv 1-rp^{n+1}(\bmod p^{n+2}), \qquad \forall r \in \mathbb{Z} \tag{1}$$

（Ⅰ） 令 $p\neq 2$，$(r,p)=1$，$u_1=s/t$ 使 $s\equiv t\equiv 1(\bmod p)$。由(1)式知，必有 i，$0\leqslant i\leqslant p-1$ 使（令 $s=1+kp$，$t=1+lp$，注意$(1-rp)^i\equiv 1\pm rpi(\bmod p^2)$，代下式即可）

$$(1-rp)^i t \equiv s(\bmod p^2)$$

同理必有 j，$0\leqslant j\leqslant p-1$，使

$$(1-rp)^{i+jp} t \equiv s(\bmod p^3)$$

$$\cdots$$

依此类推得 u_1 的 p-adic（任意）逼近式

$$(1-rp)^{i+jp+kp^2+\cdots} \equiv u_1 = \frac{s}{t}(\bmod p^\infty) \tag{2}$$

又由 $c(rp,1-rp)=1$ 知 $c(rp,(1-rp)^m)=1$，$\forall m\in\mathbb{N}$，注意 c 连续并用(2)即得

$$c(rp,u_1)=1, \qquad \forall u_1=\frac{s}{t},\ s\equiv t\equiv 1\ (\bmod p) \tag{3}$$

但 $\forall a\in\mathbb{Q}^\cdot$，$a$ 可表为 $a=p^k\dfrac{m}{n}$，$(m,p)=(n,p)=1$，于是

$$a=(1p)^k\cdot(mp)\cdot(np)^{-1}$$

由此知$\mathbb{Q}^\cdot=\langle\{rp\mid(r,p)=1\}\rangle$。因而由(3)得

$$c(x,u_1)=1, \qquad \forall x\in\mathbb{Q}^\cdot \tag{4}$$

由(4)知，若 $r\equiv s(\bmod p)$，$r'\equiv s'(\bmod p)$，$(r,p)=(r',p)=1$，令 $r_1r\equiv 1(\bmod p)$，则 $r_1s\equiv 1(\bmod p)$。于是 $c(r,r')c(r_1,r')=c(s,r')c(r_1,r')$。由此知 $c(r,r')=c(s,r')$，同理知 $c(s,r')=c(s,s')$，故

$$c(r,r')=c(s,s') \tag{5}$$

注意由上节我们已知 $K_2\mathbb{Z}_p=1$。同理由(5)知

$$c(r,r')=1, \qquad \text{当}(r,p)=(r',p)=1\text{时} \tag{6}$$

再考察 $x,y=p$ 等其他情况。令 $\lambda\in\mathbb{Z}\subset\mathbb{Q}$ 为 mod p 的原根（当然一定存在），则 $\lambda^{p-1}=\lambda^{\varphi(p)}=1$。任取 $x,y\in\mathbb{Q}^\cdot$，则 x,y 可表如 $x=p^i\lambda^j u_1$，$y=p^I\lambda^J u_1'$，其中 $u_1=s/t$，$u_1'=s'/t'$，$s\equiv t\equiv s'\equiv t'\equiv 1(\bmod p)$，于是由(4)，(6)知

$$c(x,y)=c(p,p)^{iI}c(\lambda,p)^{jI-iJ} \tag{7}$$

又由定理 25.1 知作为 $c(\ ,\ )$的导出性质，有 $c(-x,x)=1$，$c(1,x)=1$，于是有

$$c(\lambda,p)^{p-1}=c(\lambda^{p-1},p)=c(1,p)=1, \tag{8}$$
$$c(p,p)c(-1,p)=c(-p,p)=1,$$
$$c(-1,p)^2=c(1,p)=1。$$

因此,注意$-1=\lambda^{(p-1)/2}$,有

$$c(p,p)=c(-1,p)=c(\lambda,p)^{(p-1)/2}$$

再用(8)即得

$$c(p,p)^2=1 \tag{9}$$

总上并由(7),(8),(9)注意此时 $2\,|\,p-1$,即得

$$c(x,y)^{p-1}=1, \qquad \forall x,y\in \mathbb{Q}_p^{\cdot}$$

由此知 $p\neq 2$ 时欲证得 h 存在且惟一。

(Ⅱ) 令 $p=2$,只需证 $c(x,y)^2=1,\forall x,y\in \mathbb{Q}_2^{\cdot}$。

仿(Ⅰ),对任意的 $u_1=\frac{s}{t}\in \mathbb{Q}_2^{\cdot}$,其中 $s\equiv t\equiv 1(\bmod 8)$,注意,取

$$-9=1-5\cdot 2=1-rp,\ (5,2)=1$$

有

$$9^{i+j\cdot 2+k\cdot 2^2+\cdots}\equiv u_1(\bmod 2^{\infty}) \tag{10}$$

由

$$c(9,-1)=c(3,-1)^2=c(3,1)=1,$$
$$c(9,-2)=c(3,-2)^2=1\ (注意\ 3+(-2)=1),$$
$$c(9,3)=c(-3,3)^2=1\ (注意\ -3+3=0),$$

用 $c(,)$ 的连续性及(10)即得

$$c(u_1,-1)=c(u_1,-2)=c(u_1,3)=1。 \tag{11}$$

再证明:$\langle\{-1,-2,3\}\rangle<\mathbb{Q}_2^{\cdot}$ 在 $\mathbb{Q}_2^{\cdot}$ 中处处稠密(对 2-adic 拓扑)。

事实上,$\forall x\in \mathbb{Q}_2^{\cdot}$,$x=(-1)^i2^j5^ku_2$,$u_2=\frac{m}{n}$,$m\equiv n\equiv 1(\bmod 8)$,由(10)知必有 $f(2)=a_0+a_1\cdot 2+a_2\cdot 2^2+\cdots$,$a_j=0,1$,使对 2-adic 拓扑

$$9^{f(2)}\to u_2,\quad 即\ 3^{2f(2)}\to u_2。$$

又 $2=(-1)(-2)$,取 $-5/3=-15/9=s/t$,$s\equiv t\equiv 1(\bmod 8)$,同理知,有 $g(2)=b_0+b_1\cdot 2+b_2\cdot 2^2+\cdots$ 使

$$9^{g(2)}\to -\frac{5}{3}$$

因此,$3^{2g(2)+1}\to -5$,$(-1)3^{2g(2)+1}\to 5$。由此即知 $\langle\{-1,-2,3\}\rangle$ 在 $\mathbb{Q}_2^{\cdot}$ 中处处稠密。

由(11)与此稠密性以及 $c(,)$ 的连续性即知

$$c(u_1, \mathbb{Q}^{\cdot}) = 1 \tag{12}$$

取 $u_1 = -5/3$,又由(12)得

$$c(5,x) = c(-3,x), \qquad \forall x \in \mathbb{Q}^{\cdot} \tag{13}$$

取 $x=4$,则又得 $c(5,4)=c(-3,4)=1$。而 $c(5,4)=c(5,-1)c(5,-4)$,$c(5,-4)=1$,因此,$c(5,-4)=c(5,-1)=1$。但 $c(5,5)c(5,-1)=c(5,-5)=1$,于是又得

$$c(5,5) = c(5,-1) = 1 \tag{14}$$

仿上又可得 $c(-5,x)=c(3,x)$,$\forall x \in \mathbb{Q}^{\cdot}$,令 $x=-2$,则得

$$c(-5,-2) = 1 \tag{15}$$

再用(15),(14)与 $c(-1,-1)^{-1}=c(-1,-1)$ 可得

$$\begin{aligned} c(5,2) &= c(-5,2)c(-1,2) \\ &= c(-5,2) = c(-5,-2)c(-5,-1) \\ &= c(-5,-1) = c(-1,-1)c(5,-1) \\ &= c(-1,-1) = c(2,5) \end{aligned}$$

$$c(5,2)^2 = c(2,5)^2 = 1 \tag{16}$$

用 $c(2,-2)=1=c(2,-1)$,又得

$$c(2,2) = c(2,-1) = 1 \tag{17}$$

将(12),(14),(16),(17)用于 $\mathbb{Q}^{\cdot}$ 中元素的标准形,即得

$$\begin{aligned} c(x,y) &= c((-1)^i 2^j 5^k u,\ (-1)^I 2^J 5^K u') \\ &= c(-1,-1)^{iI+jK+kJ} \end{aligned}$$

而 $c(-1,-1)^2=1$,于是 $c(x,y)^2=1$,$\forall x,y \in \mathbb{Q}^{\cdot}$。这又证出在 $p=2$ 时,h 存在且惟一。 □

定义 27.2　记

$$L_m = \langle \{\{x,y\} \mid x,y \in \mathbb{Z} \text{ 且 } |x|,|y| \leqslant m\} \rangle < K_2\mathbb{Q},\ m = 1,2,\cdots$$

用此记号来证

引理 27.1　(1) $L_1 < L_2 < L_3 < \cdots$,且 $K_2\mathbb{Q} = \bigcup_{m=1,2,3,\cdots} L_m$,

(2) $L_m/L_{m-1} \simeq \begin{cases} 1, & m \text{ 非素数或 } m=2 \\ \mathbb{Z}_p^{\cdot} = A_p, & m=p \text{ 为奇素数} \end{cases}$

证　(1)是显见的。

(2) 若 $m=ab$,$1<a,b<m$,则 $|a|,|b| \leqslant m-1$,因此 $L_m \subseteq L_{m-1}$,故由(1)知 $L_m = L_{m-1}$,即 $L_m/L_{m-1}=1$。

$m=2$ 时

$\{2,2\}=\{2,-1\}\{2,-2\}=1\cdot 1=1$

$\{-2,2\}=\{2,-2\}=1$

$\{-2,-2\}=\{2,-2\}\{-1,-2\}=\{-1,-2\}=\{-1,-1\}\{-1,2\}=\{-1,-1\}$

$\{1,\pm 2\}=\{\pm 2,1\}=1$

$\{-2,-1\}=\{2,-1\}\{-1,-1\}=\{-1,-1\}=\{-1,-2\}$

由此即知 $L_2/L_1=1$。

下面只需对 $m=p$（奇素数）证明 $L_p/L_{p-1}\simeq\mathbb{Z}_p^{\cdot}$。为此作

$$\psi:\ \mathbb{Z}_p^{\cdot}\longrightarrow L_p/L_{p-1}$$

$$x\longmapsto\{x,p\}\bmod L_{p-1},\ 0<|x|\leqslant p-1$$

显然，若 ψ 是完全确定的，则必为群同态，现证 ψ 是完全确定的。为此，令 $xy\equiv z(\bmod p)$，$0<|x|,|y|,|z|\leqslant p-1$，则 $xy=z+pr$ 且

$$|pr|\leqslant|xy|+|z|\leqslant(p-1)^2+(p-1)$$

由此知 $|r|\leqslant p-1$，而由 $xy=z+pr$ 又知

$$1=\frac{z}{xy}+\frac{pr}{xy}$$

因此，注意 $pr/xy=p(r/xy)$ 得

$$1=\left\{\frac{z}{xy},\frac{pr}{xy}\right\}\equiv\left\{\frac{z}{xy},p\right\}\bmod L_{p-1}$$

即 $\{z,p\}\equiv\{xy,p\}\bmod L_{p-1}$，由此知 ψ 是完全确定的群同态。

再证 ψ 是满的，事实上，

$$L_p=\langle\{\{x,\pm p\},\{\pm p,\pm p\}\mid |x|\leqslant p\},L_{p-1}\rangle$$

但 $\{-p,p\}=\{p,-p\}=1$，又由 $\{-p,-1\}^2=\{-p,1\}=1$ 与 $\{-1,-1\}\in L_{p-1}$ 知

$$\begin{aligned}\{-p,-p\}&=\{-p,-1\}\{-p,p\}=\{-p,-1\}\\&=\{-p,-1\}^{-1}=\{-1,-p\}=\{-1,-1\}\{-1,p\}\\&=\psi(-1)\bmod L_{p-1}\end{aligned}$$

$$\begin{aligned}\{p,p\}&=\{-p,p\}\{-1,p\}=\{-1,p\}\\&=\psi(-1)\bmod L_{p-1}\end{aligned}$$

$$\begin{aligned}\{\pm p,x\}^{-1}&=\{x,\pm p\}\equiv\{x,p\}\\&=\psi(x)\bmod L_{p-1},0<|x|\leqslant p-1\end{aligned}$$

因此 ψ 是满的。由此又知

$$|L_p/L_{p-1}|\leqslant p-1\quad(\text{因为}\ |\mathbb{Z}_p^{\cdot}|=p-1)\tag{18}$$

再考察

$$h: K_2\mathbb{Q} \to A_p = \mathbb{Z}_p^{\cdot}$$
$$\{x, y\} \mapsto (x, y)_p$$

注意$|x|, |y| \leqslant p-1$ 时，$v(x)=v(y)=0$，于是$(x,y)_p=1$。因此 $h(L_{p-1})=1$。又 $h(L_p)=A_p$，于是$|L_p/L_{p-1}| \geqslant p-1$。再由(18)知$|L_p/L_{p-1}|=p-1=|\mathbb{Z}_p^{\cdot}|$，故 ψ 必为同构。 □

由此引理不难证明 Tate 关于 K_2Q 的如下优美结果。

定理 27.2(Tate)　$K_2\mathbb{Q} \simeq A_2 \oplus A_3 \oplus A_5 \oplus \cdots = \bigoplus_{\text{素数}p} A_p$，其中 $A_2=\{\pm 1\}$。$A_p=\mathbb{Z}_p^{\cdot}$，$\forall\, 2\nmid p$，p 为素数。

证　由上引理之证的末段知，$h(L_p)=A_p$，$h(L_{p-1})=1$，且

$$|L_p/L_{p-1}| = p-1 = |A_p|$$

由此即知

$$L_p/L_{p-1} \simeq A_p$$

$p=2$ 时 $L_1=\langle\{-1,-1\}\rangle$，$h(\{-1,-1\})=(-1,-1)_2=-1$，于是 $L_1=L_2\simeq A_2$。对全体素数集$\{2,3,5,\cdots\}$用归纳法。$\forall$ 素数 p，令

$$\{x, y\} \mapsto (x,y)_2 \oplus (x,y)_3 \oplus \cdots \oplus (x,y)_p$$

则知

$$L_p \simeq A_2 \oplus A_3 \oplus \cdots \oplus A_p$$

于是，再由上引理即知

$$\varinjlim_{p\to\infty} L_p = \bigcup_{\text{素数}p} L_p = K_2\mathbb{Q} \simeq A_2 \oplus A_3 \oplus A_5 \oplus \cdots = \bigoplus_{\text{素数}p} A_p \qquad \square$$

由此定理立得

推论 27.1　设 A 为任一 Abel 群，$c: \mathbb{Q}^{\cdot} \times \mathbb{Q}^{\cdot} \to A$ 对应着 Steinberg 符号 $c(,)$，则有惟一的群同态

$$\varphi_p: A_p \to A$$

使

$$c(x,y) = \prod_{\text{素数}p} \varphi_p((x,y)_p), \qquad \forall\, x, y \in \mathbb{Q}^{\cdot} \tag{19}$$

注①　此推论也可不用 K_2 群工具直接证明。

② 对$\mathbb{R}$ 定义 $c: \mathbb{R}^{\cdot} \times \mathbb{R}^{\cdot} \to \{\pm 1\}$使

$$c(u,v) = \begin{cases} 1, & u>0 \text{ 或 } v>0 \\ -1, & u<0 \text{ 且 } v<0 \end{cases}$$

则 $c(,)$为泛连续的 Steinberg 符号。

记$(u,v)_\infty = c(u,v)$，则等价地有

$$(u,v)_\infty=\begin{cases}1, & ux^2+vy^2=1\text{ 在}\mathbb{R}\text{ 中有解}(x,y)\\ -1, & ux^2+vy^2=1\text{ 在}\mathbb{R}\text{ 中无解}\end{cases}$$

这种定义可对任意特征数非2的域 F 使用。有时也记为$(,)_F$，统称为 F 上的 **Hilbert 符号**或 **Hilbert 二次剩余符号**(Hilbert quadratic residue symbol)。用于$\mathbb{Q}$，推论27.1指出了

$$(x,y)_\infty=\prod_{\text{素数}p}\varphi_p((x,y)_p),\qquad \forall x,y\in\mathbb{Q}^\cdot \tag{20}$$

这已孕育着下节将介绍的二次互反律等互反律的思想。

③ 可以证明在 $K_2\mathbb{R}$ 中$\{-1,-1\}\neq1$ 且当 $R\to S<\mathbb{R}$ 环同态存在时，在 K_2R 中也有$\{-1,-1\}\neq1$(当然$\{-1,-1\}^2=1$)。

④ 容易看出 Hilbert 符号具备双乘性与$(x,y)_\infty=1$，$\forall x,y\neq0$ 但 $x+y=1$，这正是泛 Steinberg 符号的关系集，因此带来了对 K_2 群的一系列重要的应用。

§28 二次互反律

在上节中对奇素数 p，用任意有理数 $0\neq a\in\mathbb{Q}$ 的下述表示

$$a=p^{v(a)}\frac{m}{n},\ (m,p)=(n,p)=1$$

定义了驯符号

$$(x,y)_p=(-1)^{v(x)v(y)}x^{v(y)}/y^{v(x)}(\mathrm{mod}\ p)\ (\mathbb{F}_p\text{ 中元素})$$

对素数2，用 $0\neq x,y\in\mathbb{Q}$ 的下述表示

$$x=(-1)^i2^j5^k\frac{m}{n},\ m,n\equiv1(\mathrm{mod}\ 8),$$

$$y=(-1)^I2^J5^K\frac{m'}{n'},\ m',n'\equiv1(\mathrm{mod}\ 8)。\tag{$*$}$$

定义了

$$(x,y)_2=(-1)^{iI+jK+kJ}\in\{\pm1\}=A_2$$

并证明了$(,)_p$ 与$(,)_2$ 都是$\mathbb{Q}^\cdot$ 上的 Steinberg 符号。现在取公共的值域$\{\pm1\}$将它们统一如下(注意对奇素数 p，上节已证$(x,y)_p^{p-1}\equiv1(\mathrm{mod}\ p)$，因而$(x,y)_p^{(p-1)/2}\equiv\pm1(\mathrm{mod}\ p)$)。

定义 28.1 记

$$((x,y))_p=\begin{cases}(x,y)_2, & p=2\text{ 时},\\ (x,y)_p^{(p-1)/2}(\mathrm{mod}\ p), & p\neq2\text{ 为素数时},\end{cases}\qquad\forall x,y\in\mathbb{Q}^\cdot$$

则$((x,y))_p=\pm 1$,称为 **Hilbert 符号**,

$$(x,y)_\infty=\begin{cases}1, & x>0 \text{ 或 } y>0 \text{ 时}, \\ -1, & x<0 \text{ 且 } y<0 \text{ 时}, \end{cases} \qquad x,y\in \mathbb{Q}^*$$

也称为 **Hilbert 符号**。

下面来证明关于 Hilbert 符号的二次互反(逆)律。这里的"二次",一方面指这些符号取值于二次单位根$\{\pm 1\}$,另一方面也是由于它在"二次(平方)剩余"方面有重要的应用。事实上,它也是研究数域 F 的代数整元环的 K_2 群的重要工具。

定理 28.1 **(二次互反律**(quadratic reciprocity law))

$$(x,y)_\infty=\prod_{\text{素数}p}((x,y))_p, \qquad \forall x,y\in \mathbb{Q}^*$$

即

$$(x,y)_\infty\prod_{\text{素数}p}((x,y))_p=1, \qquad \forall x,y\in \mathbb{Q}^*$$

证 在上节(20)式中取 $c(,)=(,)_\infty$,$A=\{\pm 1\}$,注意 $\varphi_p:A_p\to A$,则得

$$(x,y)_\infty=\prod_{\text{素数}p}((x,y))_p^{\varepsilon_p}, \text{其中 } \varepsilon_2,\varepsilon_3,\cdots,\varepsilon_p,\cdots,=0,1 \qquad (1)$$

只需取 x,y 的特殊值证出 $\varepsilon_2=\varepsilon_3=\cdots=\varepsilon_p=\cdots=1$ 即可。

令 $x=y=-1$ 得

$((-1,-1))_2=(-1,-1)_2=-1$

$(-1,-1)_\infty=-1$

$\forall 2\nmid p$, $((-1,-1))_p=1^{\frac{p-1}{2}}=1$(注意 $v_p(-1)=0$)

由此代入(1)得 $\varepsilon_2=1$。

再注意 $2\nmid p$ 时 $p=8k\pm 3,8k\pm 1$。

(a) 当 $p=8k\pm 3$ 时,取 $x=2,y=p$,显然$(2,p)_\infty=1$。而

$$2=(-1)^0 2^1\cdot 5^0\cdot 1,\ p=(-1)^0 2^0\cdot 5^{-1}(-3\cdot 5)$$

或

$$(-1)^1\cdot 2^0\cdot 5^{-1}(-3\cdot 5)$$

于是$(2,p)_2=1$。

再由上证的 $\varepsilon_2=1$,即得$((2,p))_2^{\varepsilon_2}=-1$。

对 $q\neq p$, $(2,p)_q=1$,因此$((2,p))_q=1$,$((2,p))_q^{\varepsilon_q}=1$。

再注意$(2,p)_p=-1$,总上代入(1)即得 $\varepsilon_p=1$。

(b) 当 $p=8k-1$ 时,$(-1,p)_\infty=1$, $(-1,p)_2=-1$,同理得 $\varepsilon_p=1$。

(c) 当 $p=8k+1$ 时,我们需先证下述引理。

引理 28.1 设 $p=8k+1$ 为素数,则有素数 $q<\sqrt{p}$使 p 不是 mod q 的

平方剩余(即 $x^2 \not\equiv p \pmod q$, $\forall x \in \mathbb{Z}_q^{\cdot}$)。

(注意条件 $p=8k+1$ 是必不可少的,比如素数 $109 \equiv 5 \not\equiv 1 \pmod 8$, $\{q \mid q<\sqrt{p}, q$ 为素数$\}=\{2,3,5,7\}$ 而 $109 \equiv 2^2 \bmod 3$, $\bmod 5$, $\bmod 7$, $109 \equiv 1^2 \bmod 2$)。

证 (J. Tate)取 $m=\max\{a \mid a<\sqrt{p}, 2\nmid a\}$,则 $m^2<p<(m+2)^2$。于是

$$0<\frac{p-i^2}{4}<\frac{(m+2)^2-i^2}{4}$$
$$=\frac{m+2+i}{2}\cdot\frac{m+2-i}{2}, \qquad i=1,3,5,\cdots,m$$

而

$$\frac{m+2+m}{2}\cdot\frac{m+2-m}{2}=(m+1)\cdot 1$$
$$\frac{m+2+m-2}{2}\cdot\frac{m+2-(m-2)}{2}=m\cdot 2$$
$$\cdots\cdots\cdots$$

因此,令 $N=\frac{p-1^2}{4}\cdot\frac{p-3^2}{4}\cdots\frac{p-m^2}{4}$,则

$$0<N<(m+1)! \tag{2}$$

若对一切满足 $q<\sqrt{p}$ 的素数,p 均为 $\bmod q$ 的平方剩余,来证 $N \equiv 0 \pmod{(m+1)!}$ 即与(2)矛盾。

为证 $a_1 \cdots a_k \equiv 0 \pmod{n!}$,只需证:对素数幂 $q^s \leqslant n$,至少有$[\frac{n}{q^s}]$个 a_j 被 q^s 整除,这里$[x]$表示不超过 x 的最大整数(这是因为

$$\sum_{\substack{y=1,2,\cdots,x \\ n \mid y}} 1=[\frac{x}{n}] \text{ 且 } n!=\prod_{q^s \leqslant n} q^{[\frac{n}{q^s}]})$$

由此知,对一切素数幂 $q^s \leqslant m+1$,只需证 $q^s \mid \frac{p-i^2}{4}$(即 $4q^s \mid (p-i^2)$)的 i 的个数至少为$[\frac{m+1}{q^s}]$,即证 $p \equiv i^2 \pmod{4q^s}$ 在$(0, m+1)$中至少有$[\frac{m+1}{q^s}]$个解。为此先证

(A) p 为 $\bmod 4q^s$ 的平方剩余。

首先注意:设 $2\nmid a$,则对 $x^2 \equiv a \pmod{2^l}$,当 $l=1$ 时有惟一解 $x \equiv 1 \pmod 2$;当 $l=2$ 时,有解$\Leftrightarrow a \equiv 1 \pmod 4$(此时两解为 $1,3 \pmod 4$);当 $l \geqslant 3$ 时,有解$\Leftrightarrow a \equiv 1 \pmod 8$(此时有 4 解)。于是由 $p \equiv 1 \pmod 8$ 知 p 为模 2^n 的平方剩余,$\forall n=1,2,\cdots$,特别地,p 为 $\bmod 4$ 的平方剩余。因此只需考虑 $2\nmid q$

的情况,但此时$(4,q^s)=1$,于是只需证 p 为 mod q^s 的平方剩余即得(A)。

事实上,由上知 $2\nmid m$,而 $m=\max\{a \mid a<\sqrt{p},2\nmid a\}$,因此 $q^s\neq m+1$。由此得 $q\leqslant q^s\leqslant m<\sqrt{p}$。由前设((2)式下一行),$p$ 为 mod q 的平方剩余,于是可令 $p\equiv x_1^2(\bmod q)$。再令 $f(x)=x^2-p$,则 $f'(x)=2x$。因而由 $p\equiv x_1^2(\bmod q)$知$(2x_1,q)=1$,即素数 $q\nmid 2x_1$,于是

$$q \mid f(x_1) \text{ 但 } q\nmid f'(x_1)$$

因此

$$f(x_1+qt_1)\equiv f(x_1)+qf'(x_1)t_1\equiv 0(\bmod q^2)$$

即

$$f(x_1)/g+f'(x_1)t_1\equiv 0\ (\bmod q)$$

有惟一解 $t_1=t_1'(\bmod q)$。由此知 $x\equiv x_1+qt_1'(\bmod q^2)$为 $p\equiv x^2(\bmod q^2)$之解,…,依此类推,即知 p 为 mod q^s 的平方剩余。从而证出了(A),即有 $i\in\mathbb{Z}$ 使 $p\equiv i^2(\bmod 4q^s)$。

(B) $p\equiv i^2(\bmod 4q^2)$在$(0,m+1)$中至少有$[\frac{m+1}{q^s}]$个解。

事实上,显然有

$$(i\pm 2q^s)^2\equiv i^2(\bmod 4q^2)$$

因此再由(A)知必有 $i_0\in\mathbb{Z}$ 使 $0<i_0<q^s$,且 $p\equiv i_0^2(\bmod 4q^2)$。因此 $p\equiv i_0^2(\bmod 4q^s)$有解 $2q^s-i_0$ 在$(q^s,2q^s)$内,有解 i_0+2q^s 在$(2q^s,3q^s)$内,…,由此知,对任意的 $n\in\mathbb{N}$,至少有$[n/q^s]$个解在$(0,n)$内,取 $n=m+1$ 即得证。□

下面接着考察定理 28.1 证明中的情况(c),即 $p=8k+1$ 的情况。

此时由上引理知,必有素数 $q<\sqrt{p}$使 p 不是 mod q 的平方剩余。我们取 $x=p,y=q$,由 $p=8k+1$ 知,素数 p 可取的最小值为 17,于是可令

$$\{p=8k+1\}=\{p_1=17<p_2<\cdots\}$$

由于小于 17 的素数为 $13(\equiv-3(\bmod 8))$, $11(\equiv 3(\bmod 8))$, $7(\equiv-1(\bmod 8))$, $5(\equiv-3(\bmod 8))$, $3(\equiv 3(\bmod 8))$及 2(前已证 $\varepsilon_2=1$),因此由前证知,$\forall$ 素数 $q<p_1,\varepsilon_q=1$。于是我们可作归纳假设:对任意的素数 $q<p,\varepsilon_q=1$,来证 $\varepsilon_p=1$ 即可。

事实上,由定义知$(p,q)_\infty=1,(p,q)_2=((p,q))_2=1$(当 $q=2$ 或 $2\nmid q$ 时),但由 $p=(-1)^0 2^0 5^0(8k+1)$,又知$(p,q)_q\equiv p^1/q^0\equiv p(\bmod q)$。而由上引理知,$\forall x\in\mathbb{Z}_q^*$,$p\not\equiv x^2(\bmod q)$,于是

$$p^{\frac{q-1}{2}}\equiv -1(\bmod q)$$

因此$((p,q))_q=-1$。由上设 $\varepsilon_q=1$ 又知

$$((p,q))_q^{\varepsilon_q} = -1$$

另一方面，对素数 $q_1 \neq q$, $q, q_1 < p$,

$$(p,q)_{q_1} \equiv p^0/q^0 \equiv 1 (\bmod q_1)$$

由此知 $((p,q))_{q_1} = 1$，因此

$$((p,q))_{q_1}^{\varepsilon_{q_1}} = 1$$

这样就从(1)式得了

$$((p,q))_p^{\varepsilon_p} = -1$$

但 $\varepsilon_p = 0$ 或 1，因此 $\varepsilon_p = 1$。 □

作为定理 28.1 的应用，我们将通过一些具体的计算推出数论中著名的二次互反律及一些其他形式的互反律。首先注意数论中模(素数) p 的一元二次同余式(方程)

$$ax^2 + bx + c \equiv 0 (\bmod p),\ (a,p) = 1$$

当 $p=2$ 时十分简单，对一般的奇素数，$(a,p)=1$ 蕴含着有 $a' \in \mathbb{Z}$ 使 $aa' = 1 (\bmod p)$。于是不失一般地可令 $a=1$，而一次项系数 b 为奇数时总可通过加上 px(不影响其解)使成偶数。因此通过配方知，研究上述的一元二次同余式归为研究

$$x^2 \equiv c (\bmod p)\text{，其中}(c,p) = 1\text{。}$$

此同余式有解时，称 c 为 mod p 的平方剩余；否则称 c 为 mod$p$ 的非平方剩余。1789 年 A. M. Legendre 引进了一种符号—Legendre 符号(其中 $a \not\equiv 0 (\bmod p)$)

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & a \text{ 为 mod } p \text{ 的平方剩余} \\ -1, & a \text{ 非 mod } p \text{ 的平方剩余} \end{cases}$$

先来验证如下引理，从中可看出，事实上，Legendre 符号即上述的 $((a,p))_p$。

引理 28.2 设 p 为奇素数，$a, b \not\equiv 0 (\bmod p)$，则

(1) $((a,b))_p = 1$;

(2) $((x,y))_p = ((y,x))_p^{-1}$(反对称性)，$\forall x, y \in \mathbb{Z}$;

(3) $((a,p))_p = \left(\frac{a}{p}\right)$，因此

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right);$$

(4) $((c,d))_2 = (c,d)_2 = (-1)^{\frac{c-1}{2}\frac{d-1}{2}}$, $\forall\, 2 \nmid c, d$,

$((c,2))_2 = (c,2)_2 = (-1)^{\frac{1}{8}(c^2-1)}$, $\forall\, 2 \nmid c$。

证　(1) 注意 $a,b\not\equiv 0 \pmod p$ 时，$v_p(a)=v_p(b)=0$，即知

$$((a,b))_p = (a,b)_p^{\frac{p-1}{2}} \pmod p = 1^{\frac{p-1}{2}} = 1$$

(2) 由 $(x,y)_p=(y,x)_p^{-1}$ 即得。

(3) 此时 $v_p(a)=0, v_p(p)=1$，因此

$$((a,p))_p = (a,p)_p^{\frac{p-1}{2}} \equiv ((-1)^0 a^1/p^0)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} \pmod p$$

而 $a^{\frac{p-1}{2}}\equiv 1 \pmod p \Leftrightarrow a$ 为 mod p 的平方剩余，于是

$$((a,p))_p = \left(\frac{a}{p}\right)$$

(4) 按本节开头的标准表示式(*)，注意：对奇数 n，$n\equiv 1,3,5,7 \pmod 8$；

$n=8k+1$ 时，$n=(-1)^0 2^0 5^0 n$，$2\mid(n-1)/2$，$2\mid(n^2-1)/8$；

$n=8k+3$ 时，$n=(-1)^1 2^0 5^{-1}(-5n)$，$(-5n\equiv 1 \pmod 8)$，$2\nmid(n-1)/2$，$2\nmid(n^2-1)/8$；

$n=8k+5$ 时，$n=(-1)^0 2^0 5^{-1}(5n)$，$(5n\equiv 1 \pmod 8)$，$2\mid(n-1)/2$，$2\nmid(n^2-1)/8$；

$n=8k+7$ 时，$n=(-1)^1 2^0 5^0(-n)$，$(-n\equiv 1 \pmod 8)$，$2\nmid(n-1)/2$，$2\mid(n^2-1)/8$。

由此知，mod 8 后验证(4)，即令 $c,d=1,3,5,7$ 去验证(4)，并不失一般性(注意对偶数不真。如 $2\equiv 10 \pmod 8$，但 $2=(-1)^0 2^1 5^0\cdot 1$，然而 $10=(-1)^0 2^1 5^1\cdot 1$，表示式并不一致)。又由定义知 $((a,b))_2=(a,b)_2=(b,a)_2$，$(1,a)_2=1$，$\forall 0\neq a,b\in\mathbb{Z}$；$(1-x,x)_2=1$，$\forall 0,1\neq x\in\mathbb{Z}$；$(a,-a)_2=1$，$\forall 0\neq a\in\mathbb{Z}$。因此 $c=1$ 或 $d=1$ 可不必考虑。于是验证 $(3,3)_2$，$(3,5)_2$，$(3,7)_2$，$(5,7)_2$ 的如下结果后，即得(4)中第一式：

$$(3,3)_2 = (-1)^{1\cdot 1+0(-1)+(-1)0} = -1 = (-1)^{\frac{3-1}{2}\cdot\frac{3-1}{2}}$$

$$(3,5)_2 = (3,-3)_2 = 1 = (-1)^{\frac{3-1}{2}\cdot\frac{5-1}{2}}$$

$$(3,7)_2 = -1 = (-1)^{\frac{3-1}{2}\cdot\frac{7-1}{2}}$$

$$(5,7)_2 = 1 = (-1)^{\frac{5-1}{2}\cdot\frac{7-1}{2}}$$

再由 $2=(-1)^0 2^1 5^0\cdot 1$ 又知

$$(3,2)_2=(-1)^{-1}=-1=(-1)^{\frac{1}{8}(3^2-1)}$$

$$(5,2)_2=(-1)^{-1}=-1=(-1)^{\frac{1}{8}(5^2-1)}$$

$$(7,2)_2=(-1)^0=1=(-1)^{\frac{1}{8}(7^2-1)}$$

这又证出了(4)的第二式。 □

作为定理28.1的推论，我们来给出数论中的二次互反律。在下面的证明中，为方便读者阅读，不用文字叙述，而只以“⇒”表示“蕴含(可推出)”，用简单的算式给出其证明。

推论 28.1 (Gauss-Legendre 二次互反(逆)律)

设 $p\neq q$ 为二奇素数，则

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}，即 \left(\frac{q}{p}\right)=(-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{p}{q}\right) \tag{3}$$

$$\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}} \tag{4}$$

$$\left(\frac{2}{p}\right)=(-1)^{\frac{1}{8}(p^2-1)} \tag{5}$$

证 定理28.1$\Rightarrow(p,q)_\infty\prod\limits_{素数r}((p,q))_r=1$。

$$\left.\begin{array}{l}p>0,q>0\Rightarrow(p,q)_\infty=1\\ \forall r\neq p,q,\ r 为奇素数 \underset{引理28.2}{\Rightarrow}((p,q))_r=1\end{array}\right\}$$

$$\Rightarrow((p,q))_p((p,q))_q((p,q))_2=1$$

$$\xrightarrow[((p,q))_2=((p,q))_2^{-1}=\pm1]{}((p,q))_p((p,q))_q=((p,q))_2$$

$$((p,q))_p=((q,p))_p^{-1}=\left(\frac{q}{p}\right)^{-1},\quad ((p,q))_q=\left(\frac{p}{q}\right),\quad ((p,q))_2=(-1)^{\frac{p-1}{2}\frac{q-1}{2}}\Rightarrow(3)$$

$$\left.\begin{array}{l}定理28.1\Rightarrow(-1,p)_\infty\prod\limits_{素数r}((-1,p))_r=1\\ p>0\Rightarrow(-1,p)_\infty=1\\ 引理28.2\Rightarrow((-1,p))_r=1,\forall r\neq p,2\nmid r\\ \qquad((-1,p))_2=(-1)^{-\frac{p-1}{2}}\\ \qquad((-1,p))_p=\left(\frac{-1}{p}\right)\end{array}\right\}\Rightarrow(4)$$

$$\left.\begin{array}{l}\text{定理 28.1} \Rightarrow (2,p)_\infty \prod\limits_{\text{素数}r} ((2,p))_r = 1 \\ p > 0 \Rightarrow (2,p)_\infty = 1 \\ \text{引理 28.2} \Rightarrow ((2,p))_r = 1, \forall r \neq p, 2 \nmid r \\ \qquad ((2,p))_2 = (2,p)_2 = (p,2)_2 = (-1)^{\frac{1}{8}(p^2-1)} \\ \qquad ((2,p))_p = \left(\dfrac{2}{p}\right)\end{array}\right\} \Rightarrow (5) \quad \square$$

如众周知，由 Lengendre 符号，推广到 Jacobi 符号(G. G. Jacobi，1804—1851)会带来计算上的方便与更广泛的应用。即令 $P = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}$，$2 \nmid P$，$(a,P)=1$，记

$$\left(\frac{a}{P}\right) = \left(\frac{a}{p_1}\right)^{\alpha_1} \left(\frac{a}{p_2}\right)^{\alpha_2} \cdots \left(\frac{a}{p_m}\right)^{\alpha_m}$$

等号(左边为 Jacobi 符号，右边为 Legendre 符号，在形式上不加区别)。容易验证 Jacobi 符号具有如下更便于计算的性质：

(i) $\left(\dfrac{1}{P}\right) = 1 = \left(\dfrac{a^2}{P}\right)$

(ii) $\left(\dfrac{a}{P}\right) = \left(\dfrac{b}{P}\right)$，$\forall a \equiv b \pmod P$

(iii) $(ab,P)=1$ 时，$\dfrac{ab}{P} = \left(\dfrac{a}{P}\right)\left(\dfrac{b}{P}\right)$

(iv) $(a,PQ)=1$ 时 $\left(\dfrac{a}{PQ}\right) = \left(\dfrac{a}{P}\right)\left(\dfrac{a}{Q}\right)$

(i)，(ii)，(iii)是 Legendre 符号性质，(iii)，(iv)是其双乘性。

可以证明 Gauss-Legendre 二次互反律也可对 Jacobi 符号使用，即

$$\left(\frac{Q}{P}\right)\left(\frac{P}{Q}\right) = (-1)^{\frac{P-1}{2}\frac{Q-1}{2}}，\text{当}(P,Q) = 1 \text{ 且 } 2 \nmid PQ \text{ 时；}$$

$$\left(\frac{-1}{P}\right) = (-1)^{\frac{P-1}{2}}；$$

$$\left(\frac{2}{P}\right)=(-1)^{\frac{p^2-1}{8}}。$$

下面给出一个更广的例注。

设 F 为域,$F(x)$为 F 上的一元有理函数域,对任意的 $F(x)$的非零元素

$$f=\frac{a_0x^n+\cdots+a_n}{b_0x^m+\cdots+b_m}$$

定义 $\deg f=n-m$(未必为正,称为 f 的次数),$f_0=a_0/b_0$ 称为 f 的首项系数,类似地记 $g\in F(x)$的首项系数为 g_0,则

$$\{f_0,g_0\}\in \mathrm{K}_2F$$

且可得到群正合列

$$1\to \mathrm{K}_2F\to \mathrm{K}_2F(x)\to \bigoplus_{0\neq p\in \operatorname{Spec}F[x]}(F[x]/p)^{\cdot}\to 1$$

仿 $\mathbb{Q}$ 中的相应定义,定义

$$(f,g)_p(\text{对 } F(x) \text{ 上的 } p\text{-adic 赋值}),\ \forall 0\neq \mathrm{f},\mathrm{g}\in F(x),$$

$$v_\infty(f)=-\deg f,$$

$$(f,g)_\infty=(-1)^{\deg f\cdot\deg g}g_0^{\deg f}/f_0^{\deg g}$$

在§18 中我们已定义了转移同态,即设 R 为(交换)环,环 S 为 R 的扩环且 $S\in$ f. g. P_Rm,$f:R\rightarrowtail S$ 为嵌入环同态,定义了转移同态 $f^*:\mathrm{K}_1S\to \mathrm{K}_1R$。现在,我们将下述三个同态

$$S^{\cdot}\to \mathrm{K}_1S\xrightarrow[f^*]{}\mathrm{K}_1R\xrightarrow[\det]{}R^{\cdot}$$

的合成称为**范同态**(norm homomorphism),并记为 norm:$S^{\cdot}\to R^{\cdot}$。用于上例得 norm:$(F[x]/p)^{\cdot}\to F^{\cdot}$,由此可得著名的 Weil 公式(见[Milnor, 1971]):

$$(f,g)^{-1}=\prod_{0\neq p\in \operatorname{Spec}F[x]}\operatorname{norm}(f,g)_p$$

当 $f,g\in F[x]$ 且$(f,g)=1$ 时,

$$(f,g)_\infty^{-1}=\prod_{g(\xi)=0}f(\xi)/\prod_{f(\eta)=0}g(\eta),$$

其中 ξ,η 为 F 的代数闭包中的元素,n 重零点作 n 次算入。

Dedekind 环在代数几何与数论中的重要性,本书已介绍过。对 Dedekind 环 R,记其分式域为 L,Tate 给出了 K_2L 的如下结果(见[Milnor, 1971]:

$$\mathrm{K}_2L=\langle\{\{a,b\}\mid a,b\in R,(a,b)=1\}\rangle$$

下面简单地介绍一下互反律对 Dedekind 环的推广,它们更概括了数论中的

有关结果($\mathbb{Z}$ 是 Dedekind 环!)。在本节的下文中,R 都表示一个 Dedekind 环。

从§22与§27,我们已经知道,若 R 为 Dedekind 环,其分式域记为 $L=Q(R)$,则对 $\forall p\in \mathrm{Max}R, R_p\in \mathrm{DVR}$,因此 p 给出 L 的一个赋值 v_p,且由理想的分解式 $(a)=p^k\cdots$,可定义 $v_p(a)=k, \forall 0\neq a\in R$,从而又得到一个非 Archimedes 赋值。记

$$V=\{v_p \mid P\in \mathrm{Max}R\},$$
$$S_\infty=\{s\mid s\notin V \text{ 为 } L \text{ 上的赋值}\},$$
$$\bar{V}=V\cup S_\infty,$$
$$L_v=L \text{ 在 } v \text{ 定义的拓扑下的完备化。}$$

对非 Archimedes 赋值 v,记

$$R_v=v \text{ 在 } L_v \text{ 中的赋值环},$$
$$U_v(t)=\{a\in L_v^\cdot \mid v(1-a)\geqslant t\},\qquad \forall t\geqslant 0$$

则

$$U_v(t)<R_v^\cdot=U(R_v)=U_v(0),\qquad \forall t\geqslant 0$$

(注意对任意环 S, $\forall x\in S^\cdot$,或有 n 使 $x^n=1$,或对一切 n, $x^n\neq 1$,在后一情况下常称 x 为∞次单位根,因此可记 $S^\cdot=\mathrm{U}(S)$)。

定义 A $\bar{V}$ 上的一个取值在 Abel 群 C 中的互反律是指满足如下两条件的反对称双乘映射 $(,)_v: L_v^\cdot\times L_v^\cdot\to C$ 的集合(collection):

(1) $(a,1-a)_v=1$, $\forall a,1-a\in L_v^\cdot$;

(2) (积公式) $\forall a,b\in L_v^\cdot$,除有限个 $v\in\bar{V}$ 外,$(a,b)_v=1$ 且 $\prod\limits_{v\in\bar{V}}(a,b)_v=1$。

若 $0\neq q\lhd R, p\in \mathrm{Max}R$,记

$$U_p(q)=U(R/pq,q/pq)\equiv\{x\in(R/pq)^\cdot \mid x\equiv 1(\mathrm{mod}\ q/pq)\}$$

则当 $p\nmid q$ 即 $p\not\supseteq q$ 时,由中国剩余定理(CRT)知

$$R/pq=R/p\oplus R/q$$

因此 $U_p(q)\simeq(R/p)^\cdot$;而当 $p\mid q$ 即 $p\supseteq q$ 时,可令 $q=p^hq'$, $(q',p)=1$。于是 $h=v_p(q)>0$ 且

$$\begin{aligned}U_p(q)&\simeq U(R/p^{h+1},p^h/p^{h+1})\\&\simeq 1+(p^h/p^{h+1})\simeq p^h/p^{h+1}\simeq R/p\end{aligned}$$

总而言之,

$$U_p(q)\simeq\begin{cases}(R/p)^\cdot\,(\text{乘法群}), & p\nmid q,\\ R/p(\text{加法群}), & p\mid q,\end{cases}\quad\forall q\lhd R, p\in \mathrm{Max}R$$

记

$$U'_p(q) = \{a \in R \mid a \notin p \text{ 且 } a \equiv 1(\text{mod } q)\}$$

若 $\chi_p: U_p(q) \to C$ 为群同态，$a \in U'_p(q)$，则记

$$\chi_p(a) \equiv \chi_p(\bar{a}),$$

其中 $\bar{a} = \{y \in (R/pq)^{\cdot}$ 且 $y \equiv a \equiv 1(\text{mod } q/pq)\} \in U_p(q)$。

定义 B R 一个取值在 Abel 群 C 中的 q-互反律是指满足下述两条件的一个集合 $\{\chi_p \mid p \in \text{Max}R$ 且 $\chi_p: U_p(q) \to C$ 为群同态$\}$：

(1) $\forall a \in U'_p(q)$，$\chi_p(a)^{v_p(1-a)} = 1$；

(2) 若 $a \equiv 1(\text{mod } q)$，$0 \neq a, b \in R$ 使 $aR + bR = R$（即 $(a)+(b)=R$），则

$$\prod_{\substack{b \in p \\ (\text{即 } p \mid b)}} \chi_p(a)^{v_p(b)} = \prod_{\substack{a \in p \\ (\text{即 } p \mid a)}} \chi_p(b)^{v_p(a)}$$

注意这里的(1)等价于 $\chi_p(U'_p(q))^{v_p(q)} = 1$，也等价于“若 $\text{Ch}(R/p) \nmid v_p(q)$，则 χ_p 平凡”。

在 § 7 中我们已介绍了 Mennicke 符号，可以证明：对 Dedekind 环，

$$q\text{- 互反律} \underset{1-1}{\leftrightarrow} \text{Mennicke 符号}$$

将上述定义用于数域 L。记

$$\mu_m = \{x \in L \mid x^m = 1\}$$

取定义 A 中的 $C = \mu_m$，则有在 $\bar{V}$ 上的互反律，即 **m 次幂互反律**（m^{th} power reciprocity law）。当 $m=2$ 即 $C = \{\pm 1\} \simeq \mathbb{Z}_2$ 时即通常的 Gauss-Legendre 二次互反律。

二次互反律在二次型的代数理论中也有重要应用，有兴趣的读者可参看[Lam，1980]。

§ 29 K_2 群的生成元与符号$\langle , \rangle$

本节中我们介绍给出 K_2 群元素的另一种符号$\langle , \rangle$，这种符号在一定程度上也便于计算且可给出局部环 K_2 群的生成系（见下节）。与符号$\{ , \}$相比，$\langle , \rangle$对一般的环将不限于对 $R^{\cdot}$ 才能使用，但计算稍繁（虽然也有一些计算公式）。为介绍$\langle , \rangle$，先回忆一下在 § 9 中对一般环 R 使用过的 $1+ab \in R^{\cdot}$，其中 $a, b \in R$（未必$\in R^{\cdot}$）。记 $\alpha = 1+ab$，我们已核验过下述恒等式

$$(1+ba)(1-b\alpha^{-1}a) = 1 - b(\alpha^{-1} + ab\alpha^{-1} - 1)a$$
$$= 1 - b((1+ab)\alpha^{-1} - 1)a = 1 =$$

$$= (1 - b\alpha^{-1}a)(1 + ba)$$

因此,记 $\beta=1+ba$,则 $\beta\in R^{\cdot}$ 且 $\beta^{-1}=1-b\alpha^{-1}a$。

下面,仿§25,§26 的办法在 St(R)中构作一个对角元素(即对 Steinberg 同态 ϕ:St(R)→E(R),象为对角矩阵的 St(R)元素)$H_{ij}(a,b)$使 $\phi(H_{ij}(a,b))=\phi(h_{ij}(\alpha))$,从而知道 $H_{ij}(a,b)h_{ij}(\alpha)^{-1}\in K_2R$,再证明此元素与足码 i,j 无关而由 a,b 惟一确定后,即可引入这个给出 K_2R 元素的符号⟨,⟩。特别地,对 $\forall a\in J(R)$或 $b\in J(R)$都可由 a,b 给出 K_2R 的元素。

先给出如下定义:

定义 29.1　设 $R\in\mathbb{R}\text{ing}$,$a,b\in R$ 使 $\alpha=1+ab\in R^{\cdot}$,记 $\beta=1+ba$ 且

$$H_{ij}(a,b) = x_{ji}(-b\alpha^{-1})x_{ij}(a)x_{ji}(b)x_{ij}(-a\beta^{-1}),\ \forall i \neq j$$

不难证明下述结果。

命题 29.1　设 $R\in\mathbb{R}\text{ing}$,$a,b\in R$ 使 $\alpha=1+ab\in R^{\cdot}$,则

(1) $\phi(H_{ij}(a,b))=\text{diag}(u_1,u_2,\cdots)$,其中 $u_i=\alpha=1+ab$,$u_j=\beta^{-1}=(1+ba)^{-1}$,$u_k=1$,$\forall k\neq i,j$;

(2) 若 $ab=ba$(即 $\alpha=\beta$),则 $\phi(H_{ij}(a,b))=\phi(h_{ij}(\alpha))$,因此

$$H_{ij}(a,b)h_{ij}(\alpha)^{-1} \in K_2R。$$

证　(1) 设 $i=1,j=2$,由引理 9.2(1)之证,已得(只写出非平凡的二阶矩阵部分)

$$\begin{pmatrix}1 & 0\\ -b & 1\end{pmatrix}\begin{pmatrix}1 & -a\\ 0 & 1\end{pmatrix}\begin{pmatrix}1+ab & 0\\ 0 & 1\end{pmatrix}\begin{pmatrix}1 & 0\\ b & 1\end{pmatrix}\begin{pmatrix}1 & a\\ 0 & 1\end{pmatrix}$$

$$= \begin{pmatrix}1 & 0\\ 0 & 1+ba\end{pmatrix}$$

由此知

$$\begin{pmatrix}1 & a\\ 0 & 1\end{pmatrix}\begin{pmatrix}1 & 0\\ b & 1\end{pmatrix} = \begin{pmatrix}\alpha & 0\\ 0 & 1\end{pmatrix}\begin{pmatrix}1 & 0\\ b & 1\end{pmatrix}\begin{pmatrix}1 & a\\ 0 & 1\end{pmatrix}\begin{pmatrix}1 & 0\\ 0 & \beta^{-1}\end{pmatrix} = \begin{pmatrix}\alpha & 0\\ b & 1\end{pmatrix}\begin{pmatrix}1 & a\beta^{-1}\\ 0 & \beta^{-1}\end{pmatrix}$$

$$= \begin{pmatrix}1 & 0\\ b\alpha^{-1} & 1\end{pmatrix}\begin{pmatrix}\alpha & 0\\ 0 & \beta^{-1}\end{pmatrix}\begin{pmatrix}1 & a\beta^{-1}\\ 0 & 1\end{pmatrix}$$

因此

$$\begin{pmatrix}1 & 0\\ -b\alpha^{-1} & 1\end{pmatrix}\begin{pmatrix}1 & a\\ 0 & 1\end{pmatrix}\begin{pmatrix}1 & 0\\ b & 1\end{pmatrix}\begin{pmatrix}1 & -a\beta^{-1}\\ 0 & 1\end{pmatrix} = \begin{pmatrix}\alpha & 0\\ 0 & \beta^{-1}\end{pmatrix}$$

即 $\phi(H_{12}(a,b))=\text{diag}(\alpha,\beta^{-1},1,1,\cdots)$。同理可证一般情况(也可用推论 25.1)。

(2) 当 $ab=ba$ 时 $\alpha=\beta$。由命题 26.1(3)即得(2)。　□

关于 $H_{ij}(a,b)$ 的计算规律，我们有下述命题。为了证明此命题先给出一条引理，事实上，此引理是命题 26.1(5)的一个很好的推广。

引理 29.1 设 $R\in\mathbb{R}\text{ing}$, $Y\in \mathrm{St}(R)$ 为单项元(即 $\phi(Y)=P(\sigma)\mathrm{diag}(\alpha_1,\alpha_2,\cdots)$)，则

$$Yx_{ij}(a)Y^{-1} = x_{\sigma(i)\sigma(j)}(\alpha_i a\alpha_j^{-1})$$

证 (1) 先设 Y 为对角元，即 σ 为恒等置换，于是 $\sigma(i)=i,\sigma(j)=j$，取足够大的 n 使 n 大于 Y 的表示式中一切 $x_{st}(b)$ 中的足码 s,t，也大于 i,j。则当 $r\geqslant n$ 时 $\alpha_r=1$。取 $w_1=w_{i,n+1}(1)w_{j,n+2}(1)$, $Y_1=w_1Yw_1^{-1}$。由命题 26.1(5)知，Y_1 的表示式中一切 $x_{st}(b)$ 中的足码 s,t 都不同于 i,j，因此 $Y_1x_{ij}(a)=x_{ij}(a)Y_1$。还可看出(不失一般地令 $i<j$)

$$\begin{aligned}\phi(Y_1) = \mathrm{diag}(&\alpha_1,\cdots,\alpha_{i-1},1,\alpha_{i+1},\cdots,\\&\alpha_{j-1},1,\alpha_{j+1},\cdots,\alpha_n,\alpha_i,\alpha_j,1,\cdots),\end{aligned}$$

因此

$$\begin{aligned}\phi(YY_1^{-1})&=\phi(h_{i,n+1}(\alpha_i)h_{j,n+2}(\alpha_j))\\&=\mathrm{diag}(1,\cdots,1,\underset{(i)}{\alpha_i},1,\cdots,1,\underset{(j)}{\alpha_j},1,\cdots,1,\underset{(n+1)}{\alpha_i^{-1}},\alpha_j^{-1},1,\cdots)。\end{aligned}$$

由此知 $YY_1\equiv h(\mathrm{mod}\ K_2R)$，其中 $h=h_{i,n+1}(\alpha_i)h_{j,n+2}(\alpha_j)$。于是(注意 K_2R 的元素为 $\mathrm{St}(R)$ 的中心元，在相似变换时可略去)

$$\begin{aligned}Yx_{ij}(a)Y^{-1}&= (YY_1^{-1})x_{ij}(a)(YY_1^{-1})^{-1}\\&= hx_{ij}(a)h^{-1} = x_{ij}(\alpha_i a\alpha_j^{-1})(\text{命题 26.1(5)})。\end{aligned}$$

(2) 设 Y 为单项元，$\phi(Y)$ 如设中表示。由于 σ 为对换之积且 $\phi(w_{st}(1))$ 对应着对换 (st)。因此必有 $w_0\in W(R)$ 使 $\phi(w_0)=P(\sigma)\mathrm{diag}(\beta_1,\beta_2,\cdots)$, $\beta_1,\beta_2,\cdots\in R^{\cdot}$。由此知 $w_0^{-1}Y$ 为对角元，可设 $\phi(w_0^{-1}y)=\mathrm{diag}(\gamma_1,\gamma_2,\cdots)$, $\gamma_1,\gamma_2,\cdots\in R^{\cdot}$。于是由(1)知

$$W_0^{-1}Yx_{ij}(a)Y^{-1}w_0 = x_{ij}(\gamma_i a\gamma_j^{-1})$$

因此

$$\begin{aligned}Yx_{ij}(a)Y^{-1}&= w_0x_{ij}(\gamma_i a\gamma_j^{-1})W_0^{-1} = x_{\sigma(i)\sigma(j)}(\beta_i\gamma_i a\gamma_j^{-1}\beta_j^{-1})\\&= x_{\sigma(i)\sigma(j)}(\alpha_i a\alpha_j^{-1})\end{aligned}$$ □

命题 29.2 设 $R\in\mathbb{R}\text{ing}$，则

(1) $H_{ij}(a,b)=H_{ji}(-b,-a)^{-1}$, $\forall a,b\in R$ 且 $1+ab\in R^{\cdot}$；

(2) $H_{ij}(a,b+c+bac)=H_{ij}(a,b)H_{ij}(a\beta^{-1},\beta c)$, $\forall a,b,c\in R$ 且 $1+ab,1+ac\in R^{\cdot}$，其中 $\beta=1+ba$；

(3) $H_{ij}(a,bc)^{-1}H_{jk}(b,ca)^{-1}H_{ki}(c,ab)^{-1}=1$, ($\forall a,b,c\in R$ 且 $1+abc\in R^{\cdot}$)。即此时

$$H_{ki}(c,ab)H_{jk}(b,ca)H_{ij}(a,bc)=1$$

证　(1) 由 $1+(-b)(-a)=1+ba\in R^{\cdot}$ 与 $H_{ij}(a,b)$的定义即得(1)。

(2) 由

$$1+a(b+c+bac)=(1+ab)(1+ac)\in R^{\cdot},$$

$$1+(a\beta^{-1})(\beta c)=1+ac\in R^{\cdot}$$

知(2)中各项都有定义。记 $\gamma=1+ac,\delta=1+ca$，则 $1+a(b+c+bac)=\alpha\gamma,1+(b+c+bac)a=\beta\delta$，且

$$H_{ij}(a,b+c+bac)=x_{ji}(-(b+c+bac)\gamma^{-1}\alpha^{-1})x_{ij}(a)x_{ji}(b+c+bac)x_{ij}(-a\delta^{-1}\beta^{-1})$$

于是

$$\begin{aligned}
&x_{ji}((b+c+bac)\gamma^{-1}\alpha^{-1})H_{ij}(a,b+c+bac)x_{ij}(a\delta^{-1}\beta^{-1})\\
&=x_{ij}(a)x_{ji}(b+c+bac)=x_{ij}(a)x_{ji}(b+\beta c)\\
&=x_{ij}(a)x_{ji}(b)x_{ji}(\beta c)\\
&=x_{ji}(b\alpha^{-1})H_{ij}(a,b)x_{ij}(a\beta^{-1})x_{ji}(\beta c)\\
&=x_{ji}(b\alpha^{-1})H_{ij}(a,b)x_{ji}(\beta c\gamma^{-1})H_{ij}(a\beta^{-1},\beta c)x_{ij}(a\delta^{-1}\beta^{-1})\\
&=x_{ji}(b\alpha^{-1}+c\gamma^{-1}\alpha^{-1})H_{ij}(a,b)H_{ij}(a\beta^{-1},\beta c)x_{ij}(a\delta^{-1}\beta^{-1})
\end{aligned}$$

(对于对角元 $H_{ij}(a,b)$用上引理)。注意 $1+(a\beta^{-1})(\beta c)=\gamma,1+(\beta c)(a\beta^{-1})=\beta\delta\beta^{-1}$。再由上命题及

$$b\alpha^{-1}+c\gamma^{-1}\alpha^{-1}=(b\gamma+c)\gamma^{-1}\alpha^{-1}=(b+c+bac)\gamma^{-1}\alpha^{-1}$$

即得(2)。

(3) 由 $1+abc\in R^{\cdot}$ 知 $1+cab=1+c(ab)\in R^{\cdot},1+bca\in R^{\cdot}$，因此(3)中各项都有定义。

用 Philip Hall(1904－1982)的换位子恒等式

$$x[[x^{-1},z],y]x^{-1}\cdot y[[y^{-1},x],z]y^{-1}\cdot z[[z^{-1},y],x]z^{-1}=1 \qquad (1)$$

令 $x=x_{ij}(a),y=x_{ki}(c),z=x_{jk}(b),d=(1+abc)^{-1}-1,e=(1+cab)^{-1}-1,f=(1+bca)^{-1}-1$，则

$$\begin{aligned}
[[x^{-1},z],y]&=[[x_{ij}(-a),x_{jk}(b)],x_{ki}(c)]=[x_{ik}(-ab),x_{ki}(c)]\\
&=x_{ik}(-ab)x_{ki}(c)x_{ik}(ab)x_{ki}(-c)\\
&=x_{ik}(abe)H_{ki}(c,ab)x_{ki}(cd)
\end{aligned}$$

同理

$$[[y^{-1},x],z]=x_{kj}(caf)H_{jk}(b,ca)x_{jk}(be)$$

$$[[z^{-1},y],x]=x_{ji}(bca)H_{ij}(a,bc)x_{ij}(af)$$

再注意 $cda=caf$，于是

$$x_{ki}(cd)x_{ij}(-a)x_{ki}(c)x_{kj}(caf) = x_{ij}(-a)x_{ki}(cd+c) \tag{2}$$

同理有

$$x_{jk}(be)x_{ki}(-c)x_{jk}(b)x_{ji}(bcd) = x_{ki}(-c)x_{jk}(be+b) \tag{3}$$

$$x_{ij}(af)x_{jk}(-b)x_{ij}(a)x_{ik}(abe) = x_{jk}(-b)x_{ij}(af+a) \tag{4}$$

将以上各式代入(1)式得

$$x_{ij}(a)x_{ik}(abe)H_{ki}(c,ab)\underbrace{(x_{ki}(cd)x_{ij}(-a)x_{ki}(c)x_{kj}(caf))}_{(2)_{左}}\cdot$$

$$H_{jk}(b,ca)\underbrace{(x_{jk}(be)x_{ki}(-c)x_{jk}(b)x_{ji}(bcd))}_{(3)_{左}}H_{ij}(a,bc)x_{ij}(af)x_{jk}(-b)=1$$

注意在群中 $XY=1$ 时，$Y=X^{-1}$，因此 $YX=1$。将此式前两项移到左端末，并将 $(2)_{左}$，$(3)_{左}$ 分别换上 $(2)_{右}$，$(3)_{右}$ 则得

$$H_{ki}(c,ab)(2)_{右}\ H_{jk}(b,ca)(3)_{右}\ H_{ij}(a,bc)\cdot$$
$$\underbrace{(x_{ij}(af)x_{jk}(-b)x_{ij}(a)x_{ik}(abe))}_{(4)_{左}}=1$$

将 $(4)_{左}$ 换成 $(4)_{右}$，即

$$H_{ki}(c,ab)x_{ij}(-a)x_{ki}(cd+c)H_{jk}(b,ca)x_{ki}(-c)\cdot$$
$$x_{jk}(be+b)H_{ij}(a,bc)x_{jk}(-b)x_{ij}(af+a) = 1 \tag{5}$$

又由命题 29.1 及 $H_{ij}(,)$ 的定义知

$$H_{ki}(c,ab)x_{ij}(-a) = x_{ij}((1+abc)^{-1}(-a))H_{ki}(c,ab)$$

但由 $(1+abc)a=a(1+bca)$ 及 $f=(1+bca)^{-1}-1$ 知

$$(1+abc)^{-1}a = a(1+bca)^{-1} = a(f+1) = af+a$$

于是

$$x_{ij}(af+a)H_{ki}(c,ab)x_{ij}(-a) = H_{ki}(c,ab)$$

同理知

$$x_{ki}(cd+c)H_{jk}(b,ca)x_{ki}(-c) = H_{jk}(b,ca)$$

$$x_{jk}(be+b)H_{ij}(a,bc)x_{jk}(-b) = H_{ij}(a,bc)$$

将此三式代入(5)即得(3)。 □

命题 29.3 设 $R\in\mathbb{R}\mathrm{ing}$，$a,b\in R$ 使 $1+ab=\alpha\in R^{\cdot}$ 且 $ab=ba$，$i\neq j$，$k\neq l$，则

$$H_{ij}(a,b)h_{ij}(\alpha)^{-1} = H_{kl}(a,b)h_{kl}(\alpha)^{-1}$$

即 K_2R 中的元素 $H_{ij}(a,b)h_{ij}(\alpha)^{-1}$ 由 a,b 惟一确定与足码 i,j 的选取无关。

证 由推论 25.1 知，可取适当的 $w_s(u)$ 作“相似变换”把欲证的左端变成右端。但由命题 29.1 知 $H_{ij}(a,b)h_{ij}(\alpha)^{-1}\in K_2R=C(\mathrm{St}(R))$。因此左

端在此变换下不变,这就证出了 $H_{ij}(a,b)h_{ij}(\alpha)^{-1}$ 与 i,j 无关,是由 a,b 惟一确定的。 □

由此命题可给出 $\langle,\rangle$ 的如下定义。

定义 29.2　设 $R\in\mathbb{R}\text{ing}, a,b\in R$ 使 $1+ab=\alpha\in R^{\cdot}$ 且 $ab=ba$,定义 Dennis-Stein 符号

$$\langle a,b\rangle = H_{ij}(a,b)h_{ij}(\alpha)^{-1}$$

由此定义可得

命题 29.4　设 $R\in\mathbb{R}\text{ing}, a,b\in R$ 使 $1+ab=\alpha\in R^{\cdot}$ 且 $ab=ba, \gamma\in R^{\cdot}$ 使 $\alpha\gamma=\gamma\alpha$,则

(1) $\langle a\gamma^{-1},\gamma b\rangle=\langle a,b\rangle\{\alpha,\gamma\}$,即

$$\{\alpha,\gamma\} = \langle a,b\rangle^{-1}\langle a\gamma^{-1},\gamma b\rangle = \langle a\gamma^{-1},\gamma b\rangle\langle a,b\rangle^{-1};$$

(2) $\langle\{\{\alpha,\gamma\}\mid\alpha\gamma=\gamma\alpha,\alpha,\gamma\in R^{\cdot}\}\rangle\subseteq\langle\{\langle a,b\rangle\mid a,b\in R$ 使 $1+ab\in R^{\cdot}, ab=ba\}\rangle$,因此 $R\in\mathbb{C}\text{Ring}$ 时,$\{,\}$ 生成的群(K_2R 的子群)为 $\langle,\rangle$ 生成的群(也是 K_2R 的子群)的子群。

证　(1) 注意 $h_{ij}(u)=w_{ij}(u)w_{ij}(-1), \alpha=\beta$,用推论 25.1 可得

$$\begin{aligned}
&h_{23}(\gamma)H_{12}(a,b)h_{23}(\gamma)^{-1}\\
&\quad= h_{23}(\gamma)x_{21}(-b\alpha^{-1})x_{12}(a)x_{21}(b)x_{12}(-a\alpha^{-1})h_{23}(\gamma)^{-1}\\
&\quad= x_{21}(-\gamma b\alpha^{-1})x_{12}(a\gamma^{-1})x_{21}(\gamma b)x_{12}(-a\gamma^{-1}\alpha^{-1})\\
&\quad= H_{12}(a\gamma^{-1},\gamma b) \qquad (6)
\end{aligned}$$

$$h_{23}(\gamma)h_{12}(\alpha)h_{23}(\gamma)^{-1} = h_{12}(\alpha\gamma^{-1})h_{12}(\gamma^{-1})^{-1}$$

但 $\langle a,b\rangle\in K_2R=C(\mathrm{St}(R))$,于是

$$\begin{aligned}
\langle a,b\rangle &= h_{23}(\gamma)\langle a,b\rangle h_{23}(\gamma)^{-1}\\
&= h_{23}(\gamma)H_{12}(a,b)h_{12}(\alpha)^{-1}h_{23}(\gamma)^{-1}\\
&= h_{23}(\gamma)H_{12}(a,b)h_{23}(\gamma)^{-1}\cdot h_{23}(\gamma)h_{12}(\alpha)^{-1}h_{23}(\gamma)^{-1}\\
&\overset{(6)}{=\!=} H_{12}(a\gamma^{-1},\gamma b)h_{12}(\gamma^{-1})h_{12}(\alpha\gamma^{-1})^{-1}\\
&= \langle a\gamma^{-1},\gamma b\rangle\{\gamma^{-1},\alpha\}^{-1} \quad (\text{用}\langle,\rangle,\{,\}\text{定义})\\
&= \langle a\gamma^{-1},\gamma b\rangle\{\alpha,\gamma\}^{-1}
\end{aligned}$$

这就证出了(1)。

(2) 注意 $\alpha=1+(\alpha-1)\cdot 1$, $\{\alpha,\gamma\}=\langle\alpha-1,1\rangle^{-1}\langle(\alpha-1)\gamma^{-1},\gamma\rangle$ 即得。

□

对于 $\{,\}$ 与 $\langle,\rangle$ 的关系,我们有

命题 29.5　设 $R\in\mathbb{R}\text{ing}, a,b\in R$ 使 $1+ab=\alpha\in R^{\cdot}$ 且 $ab=ba$,则

(1) $\langle a,b\rangle=\begin{cases}1, & b=0 \text{ 时}\\ \{\alpha,b\}, & b\in R^{\cdot} \text{ 时}\end{cases}$

(2) $\langle a,b\rangle=\begin{cases}1, & a=0 \text{ 时}\\ \{-a,\alpha\}, & a\in R^{\cdot}\end{cases}$

证 (A) $b=0$ 时，$\alpha=1$，于是

$$\begin{aligned}\langle a,b\rangle &= H_{ij}(a,0)h_{ij}(1)^{-1}\\ &= H_{ij}(a,0)\\ &= x_{ji}(0)x_{ij}(a)x_{ji}(0)x_{ij}(-a)\\ &= 1\end{aligned}$$

(B) $b=1$ 时，$a=\alpha-1$，

$$\begin{aligned}h_{12}(\alpha) &= w_{12}(\alpha)w_{12}(-1)\\ &= x_{12}(\alpha)x_{21}(-\alpha^{-1})(x_{12}(\alpha)x_{12}(-1))x_{21}(1)x_{12}(-1)\\ &= x_{12}(\alpha)x_{21}(-\alpha^{-1})x_{12}(\alpha-1)x_{21}(1)x_{12}(-1)\end{aligned}$$

$$\begin{aligned}H_{12}(a,b) &= H_{12}(a,1) = H_{12}(\alpha-1,1)\\ &= x_{21}(-\alpha^{-1})x_{12}(\alpha-1)x_{21}(1)x_{12}(\alpha^{-1}-1)\\ &= x_{12}(-\alpha)h_{12}(\alpha)x_{12}(\alpha^{-1})\end{aligned}$$

因此

$$\begin{aligned}\langle a,b\rangle=\langle a,1\rangle &= H_{12}(a,1)h_{12}(\alpha)^{-1}\\ &= x_{12}(-\alpha)h_{12}(\alpha)x_{12}(\alpha^{-1})h_{12}(\alpha)^{-1}\\ &\overset{}{\underset{\S 26}{=\!=}} x_{12}(-\alpha)x_{12}(\alpha(\alpha^{-1})\cdot(\alpha^{-1})^{-1})\\ &= x_{12}(-\alpha)x_{12}(\alpha) = 1\end{aligned}$$

(C) 由命题 29.2(1)知 $H_{ij}(a,b)=H_{ji}(-b,-a)^{-1}$。再由推论 26.1 知 $h_{ij}(\alpha)=h_{ji}(\alpha)^{-1}$。因此

$$\begin{array}{l}\langle a,b\rangle h_{12}(\alpha) = h_{21}(\alpha)^{-1}\langle -b,-a\rangle^{-1} = h_{12}(\alpha)\langle -b,-a\rangle^{-1}\\ \quad\Vert\\ h_{12}(\alpha)\langle a,b\rangle\end{array}$$

于是$\langle a,b\rangle=\langle -b,-a\rangle^{-1}$。由此知，$a=0$ 时

$$\langle a,b\rangle=\langle -b,-a\rangle^{-1}=\langle -b,0\rangle^{-1}\underset{(A)}{=\!=}1^{-1}=1$$

(D) $b\in R^{\cdot}$ 时可令 $\gamma=b^{-1}$。于是由命题 29.4(1)知

$$\langle a\gamma^{-1},\gamma b\rangle = \langle a,b\rangle\{\alpha,\gamma\} = \langle a,b\rangle\{\alpha,b^{-1}\}$$
$$\|$$
$$\langle ab,1\rangle \overset{}{\underset{(B)}{=\!=}} 1$$

因此
$$\langle a,b\rangle = \{\alpha,b^{-1}\}^{-1} = \{\alpha,b\}$$

(E) $a\in R^{\cdot}$ 时 $-a\in R^{\cdot}$，由上证之(C)，(D)即知
$$\langle a,b\rangle = \langle -b,-a\rangle^{-1} = \{\alpha,-a\}^{-1} = \{-a,\alpha\}$$

由上证顺便得到

推论 29.1　设 $R\in\mathcal{R}\text{ing}$，$a,b\in R$，使 $1+ab=\alpha\in R^{\cdot}$ 且 $ab=ba$，则
$$\langle 0,\pm b\rangle = \langle \pm a,0\rangle = \langle \pm a,1\rangle = \langle -1,\pm b\rangle = 1$$

因此 $h_{ij}(u)=H_{ij}(u-1,1)$，$\forall u\in R^{\cdot}$，$i\neq j$。

$\langle,\rangle$的运算规律可见如下命题。

命题 29.6　设 $R\in\mathcal{R}\text{ing}$，则

(1) $\langle a,b\rangle=\langle -b,-a\rangle^{-1}$，当 $a,b\in R$ 使 $1+ab\in R^{\cdot}$ 且 $ab=ba$ 时；

(2) $\langle a,b\rangle\langle a,c\rangle=\langle a,b+c+bac\rangle$，当 $a,b,c\in R$ 使 $1+ab,1+ac\in R^{\cdot}$，且 $ab=ba,ac=ca$ 时；

(3) $\langle a,bc\rangle\langle b,ca\rangle\langle c,ab\rangle=1$，当 $a,b,c\in R$ 使 $1+abc\in R^{\cdot}$ 且 $abc=bca=cab$ 时。

证　(1) 已由命题 29.5 之证中的(C)给出。

(2) 记 $\alpha=1+ab,\gamma=1+ac$，则 $\alpha\gamma=1+a(b+c+bac)$。因此

$$\langle a,b+c+bac\rangle h_{12}(\alpha\gamma) = H_{12}(a,b+c+bac)$$
$$\underset{\text{命题 29.2(2)}}{=\!=\!=\!=} H_{12}(a,b)H_{12}(a\alpha^{-1},\alpha c) \tag{7}$$

又$(7)_{右}$中的第二个因子
$$H_{12}(a\alpha^{-1},\alpha c) = x_{21}(-\alpha c\gamma^{-1})x_{12}(a\alpha^{-1})$$
$$x_{21}(\alpha c)x_{12}(-a\alpha^{-1}(1+\alpha ca\alpha^{-1})^{-1})$$

再注意到
$$\begin{aligned}-a\alpha^{-1}(1+\alpha ca\alpha^{-1})^{-1} &= -a\alpha^{-1}(1-\alpha c\gamma^{-1}a\alpha^{-1})\\ &= -a\alpha^{-1}+ac\gamma^{-1}a\alpha^{-1}\\ &= -a(1-c\gamma^{-1}a)\alpha^{-1}\\ &= -a\gamma^{-1}\alpha^{-1}\end{aligned}$$

则由命题 26.1(5)(取 $w=h_{23}(\alpha)$)得
$$H_{12}(a\alpha^{-1},\alpha c) = x_{21}(-\alpha c\gamma^{-1})x_{12}(a\alpha^{-1})x_{21}(\alpha c)x_{12}(-a\gamma^{-1}\alpha^{-1})$$

$$= (h_{23}(\alpha)x_{21}(-c\gamma^{-1})h_{23}(\alpha)^{-1})(h_{23}(\alpha)x_{12}(a)h_{23}(\alpha)^{-1}) \cdot$$
$$(h_{23}(\alpha)x_{21}(c)h_{23}(\alpha)^{-1})(h_{23}(\alpha)x_{12}(-a\gamma^{-1})h_{23}(\alpha)^{-1})$$
$$= h_{23}(\alpha)x_{21}(-c\gamma^{-1})x_{12}(a)x_{21}(c)x_{12}(-a\gamma^{-1})h_{23}(\alpha)^{-1}$$
$$= h_{23}(\alpha)H_{12}(a,c)h_{23}(\alpha)^{-1}$$
$$= h_{23}(\alpha)\langle a,c\rangle h_{12}(\gamma)h_{23}(\alpha)^{-1}$$
$$= \langle a,c\rangle h_{23}(\alpha)h_{12}(\gamma)h_{23}(\alpha)^{-1}$$

（注意$\langle a,c\rangle \in K_2R=C(St(R))$）。

因此

$$(7)_{右} = \langle a,b\rangle\langle a,c\rangle h_{12}(\alpha)h_{23}(\alpha)h_{12}(\gamma)h_{23}(\alpha)^{-1}$$
$$= \langle a,b\rangle\langle a,c\rangle h_{12}(\alpha)h_{12}(\gamma\alpha)h_{12}(\alpha)^{-1}$$
$$= \langle a,b\rangle\langle a,c\rangle h_{12}(\alpha\gamma\alpha\alpha^{-1})h_{12}(\alpha\alpha^{-1})^{-1}$$
$$(\text{注意 } h_{12}(\alpha\alpha^{-1})^{-1} = h_{12}(1)^{-1} = 1)$$
$$= (7)_{左} = \langle a,b+c+bac\rangle h_{12}(\alpha\gamma)$$

这就证出了(2)。

(3) 由命题 29.2(3)已知 $H_{31}(c,ab)H_{23}(b,ca)H_{12}(a,bc)=1$

令 $\delta=1+abc$，注意 $abc=bca=cab$，则得

$$\langle c,ab\rangle h_{31}(\delta)\langle b,ca\rangle h_{23}(\delta)\langle a,bc\rangle h_{12}(\delta) = 1$$

由于$\langle\,,\rangle$都是 $St(R)$的中心元素，于是有

$$\langle a,bc\rangle\langle b,ca\rangle\langle c,ab\rangle h_{31}(\delta)h_{23}(\delta)h_{12}(\delta) = 1$$

但由 § 26 式(2)知 $h_{jk}(u)=h_{1k}(u)h_{1j}(u)^{-1}$，因此有

$$h_{31}(\delta)h_{23}(\delta)h_{12}(\delta)$$
$$= (h_{31}(\delta)h_{13}(\delta))(h_{12}(\delta)^{-1}h_{12}(\delta)) = 1 \cdot 1 = 1$$

这又证出了(3)。 □

为方便下面的讨论，先给出如下定义：

定义 29.3 设 $R\in \mathbb{R}\mathrm{ing}$，以

生成系：$\{\{u,v\} \mid u,v\in R^{\cdot}$ 且 $uv=vu\}$

关系集：$\{u_1,v_1v_2\}=\{u_1,v_1\}\{u_1,v_2\}$

$\{u_1u_2,v_1\}=\{u_1,v_1\}\{u_2,v_1\}$（双乘性）($\forall u_i,v_j\in R^{\cdot}$ 且 $u_iv_j=v_ju_i$)，

$\{u,1-u\}=1$, $\forall u,1-u\in R^{\cdot}$

确定的 Abel 群，记为 $MG(R)$。以

生成系：$\{\langle a,b\rangle \mid a,b\in R$ 且 $1+ab\in R^{\cdot}, ab=ba\}$

关系集：$\langle 1\rangle\langle a,b\rangle=\langle -b,-a\rangle^{-1}$ ($\forall a,b\in R$ 且 $1+ab\in R^{\cdot}, ab=ba$)

〈2〉 $\langle a,b\rangle\langle a,c\rangle=\langle a,b+c+bac\rangle$ ($\forall a,b,c\in R$ 且 $1+ab,1+ac\in R^{\cdot}$, $ab=ba,ac=ca$)

〈3〉 $\langle a,bc\rangle\langle b,ca\rangle\langle c,ab\rangle=1$ ($\forall a,b,c\in R$ 且 $1+abc\in R^{\cdot}$, $abc=bca=cab$)

确定的 Abel 群记为 $\langle MG\rangle(R)$。

对于域 R,我们可证(注意这里的〈,〉未必是定义 29.2 给出的,不能直接用命题 29.5)

定理 29.1　设 R 为域,则

$$K_2(R)\simeq MG(R)\simeq\langle MG\rangle(R)$$

证　由 Matsumoto 定理知 $K_2R\simeq MG(R)$,下面只需证 $MG(R)\simeq\langle MG\rangle(R)$,分如下几步进行证明。

(1) $\forall\{u,v\}\in MG(R)$,可设 $u\neq 1$($u=1$ 时 $\{1,v\}=1$),取 $y=v,x=-(1-u)v^{-1}$,则 $1+xy=u\in R^{\cdot}$,按命题 29.5(1)作同态

$$f:\langle MG\rangle(R)\to MG(R),$$

$$\langle a,b\rangle\mapsto\begin{cases}1, & b=0\\ \{\alpha,b\}, & b\neq 0,\text{其中 }\alpha=1+ab(\in R^{\cdot})\end{cases}$$

则 $f(\langle x,y\rangle)=\{1+xy,y\}=\{u,v\}$。证出下述的(2),即知 f 为完全确定的群(满)同态。

(2) $\{\langle a,b\rangle\}$的关系〈1〉,〈2〉,〈3〉可由它们在 f 下的象用 $MG(R)$的关系集导出。

事实上,可直接检验(为简单起见,将 $f(\langle x,y\rangle)=\{u,v\}$ 记为 $\langle x,y\rangle=\{u,v\}$):

〈1〉 $\langle a,b\rangle\langle -b,-a\rangle=\left\{\begin{matrix}1,a=0\text{ 或 }b=0,\\ \{\alpha,b\}\{\alpha,-a\}=\{\alpha,-ab\}=1\end{matrix}\right\}=1$

〈2〉 $a=0$ 时 $\langle a,b\rangle\langle a,c\rangle=\{1,b\}\{1,c\}=1\cdot 1=1=\langle a,b+c+bac\rangle$

$b=0$ 时 $\langle a,b\rangle\langle a,c\rangle=1\cdot\langle a,c\rangle=\langle a,c\rangle=\langle a,b+c+bac\rangle$

同理 $c=0$ 时〈2〉成立。

下设 $abc\neq 0$,则

$$\begin{aligned}(\langle a,b\rangle\langle a,c\rangle)^{-1}&\overset{\langle 1\rangle}{=\!=}\langle -c,-a\rangle\langle -b,-a\rangle\\&=\{1+ac,-a\}\{1+ab,-a\}\\&=\{(1+ac)(1+ab),-a\}\\&=\{1+a(b+c+bac),-a\}\\&=\langle -(b+c+bac),-a\rangle\end{aligned}$$

$$\xlongequal[\langle 1\rangle]{} \langle a, b+c+bac\rangle^{-1}$$

即〈2〉成立。

〈3〉 当 $a=0$ 或 $b=0$ 或 $c=0$ 时,〈3〉显然成立。

当 $abc\neq 0$ 时(注意 R 为域,a,b,c 对乘法是交换的)

$$\begin{aligned}\langle a,bc\rangle\langle b,ac\rangle\langle c,ab\rangle &= \{1+abc,bc\}\{1+abc,ac\}\{1+abc,ab\}\\ &= \{1+abc,(abc)^2\}\\ &= \{1+abc,-abc\}^2 = 1^2 = 1\end{aligned}$$

(3) 若有 A,B(〈MG〉(R)生成元之积)$\in$〈MG〉(R),使 $f(A)=f(B)$,即 $f(A)f(B)^{-1}=1$,由上证知 $AB^{-1}=1$(〈MG〉(R)中),即 $A=B$。由此知同态 f 为单同态,因此为群同构。 □

建议读者找出 f 的逆映射 g 且证:$MG(R)$ 的关系集可以通过这个 g,由〈MG〉(R)的关系导出。从而断言 g 为群同态,因此 f 为群同构。

注① 不难证明,作为关系集,定义 29.3 中的〈1〉,〈2〉,〈3〉等价于〈1〉,〈2〉′,〈3〉′,也等价于〈1〉,〈2〉′,〈3〉″,其中

〈2〉′::$\langle a,c\rangle\langle b,c\rangle=\langle a+b+acb,c\rangle$;

〈3〉′: $\langle a,bc\rangle=\langle ab,c\rangle\langle ac,b\rangle$;

〈3〉″: $\langle -ab,c\rangle\langle -ac,b\rangle\langle -bc,a\rangle=1$。

此外,若记 $\langle a,b\rangle_1\equiv\langle -a,b\rangle$, $\forall a,b\in R$ 且使 $1-ab\in R^{\cdot}$, $ab=ba$,则可证:

$\langle 1\rangle_1$: $\langle a,b\rangle_1=\langle b,a\rangle_1$;

$\langle 2\rangle_1$: $\langle a,b\rangle_1\langle a,c\rangle_1=\langle a,b+c-bac\rangle_1$;

$\langle 3\rangle_1$: $\langle a,bc\rangle_1\langle b,ca\rangle_1\langle c,ab\rangle_1=1$。

在下节我们将证:

1. 设 R 为交换局部环,则

$$\mathrm{K}_2R=\langle\{\langle a,b\rangle \mid a,b\in R \text{ 且 } 1+ab\in R^{\cdot}\}\rangle$$

因此为〈MG〉(R)的商群;

2. 设 R 为交换环,$I\lhd R$ 使 $I\subseteq J(R)$,$S=R/I$,且

$$\mathrm{K}_2S=\langle\{S^{\cdot},S^{\cdot}\}\rangle \text{ 或}$$

$$\mathrm{K}_2S=\langle\{\langle a',b'\rangle \mid a',b'\in S \text{ 且 } 1+a'b'\in S^{\cdot}\}\rangle$$

时,

$$\mathrm{K}_2R=\langle\{\langle a,b\rangle \mid a,b\in R \text{ 且 } 1+ab\in R^{\cdot}\}\rangle$$

因此为〈MG〉(R)的商群。

事实上,还可证(见 Silvester,1981]):设 R 为半局部环且 $R^{\cdot}\in\mathcal{A}\mathrm{G}$(比如 R 为交换的半局部环),则 $\mathrm{K}_2R=\langle\{R^{\cdot},R^{\cdot}\}\rangle$。

§30　局部环的 K_2 群

局部环的最佳性质之一是：不在其极大左（右）理想中的元素均可逆。在这个意义下来说，局部环是最接近除环及域（它们的极大理想为 0）的环类，在定义 $H_{ij}(a,b)$ 及 $\langle a,b\rangle$ 时都要求的条件"$1+ab\in R^{\cdot}$"最容易满足。事实上，我们可给出下面更一般的引理。值得注意的是，引理中在 R 的 Jacobson 根 $J(R)$ 中的理想 I 常被称为**根理想**（radical ideal）。事实上这与通常定义的根理想是不同的。通常我们定义 R 的理想 I 的根为

$$\sqrt{I}=\bigcap_{I\subset P\in \operatorname{Spec}R}P$$

（对交换环 R）当 $\sqrt{I}=I$ 时称 I 为根理想，这是代数几何中的一个重要概念，显然素理想都是根理想，$\sqrt{0}$ 常被记为 $N(R)$ 称为 R 的**素根**（一切素理想之交）。可以看出：$N(R)\subseteq J(R)$（一切极大理想之交），因此常称 $N(R)$ 为 R 的小根，而称 $J(R)$ 为 R 的大根。$I\subseteq N(R)$ 时，$\sqrt{I}=I$，$I\subseteq J(R)$ 时未必有 $\sqrt{I}=I$。同时 $\sqrt{I}=I$ 时也未必有 $I\subseteq J(R)$。基于上述现象，我们将不称 $J(R)$ 中的理想为根理想（虽然本书上面多次用过这种理想）。

引理 30.1　设 $R\in\mathfrak{R}\mathrm{ing}$，$I\lhd R$ 且 $I\subseteq J(R)$，则当 $a\in I$ 或 $b\in I$ 时 $1+ab\in R^{\cdot}$。因此，当 R 为局部环（惟一极大左（右）理想为 $\mathfrak{m}$）时，$a\in\mathfrak{m}$ 或 $b\in\mathfrak{m}$ 时，$1+ab\in R^{\cdot}$。

证　注意 $a\in I$ 或 $b\in I$ 时 $ab\in I\subseteq J(R)$，即知 $1+ab\in R^{\cdot}$。 □

定义 30.1　设 $R\in\mathfrak{R}\mathrm{ing}$，$I\lhd R$，记 $\mathrm{St}(R)$ 的子群

$$\Xi(R,I)=\langle\{H_{ij}(a,b)\mid i\neq j,a\in I,b\in R\text{ 使 }1+ab\in R^{\cdot}\}\rangle,$$
$$\Xi(R)=\Xi(R,R)。$$

显然有

命题 30.1　设 $R\in\mathfrak{R}\mathrm{ing}$，$I\lhd R$ 且 $I\subseteq J(R)$，则

$$\Xi(R,I)=\langle H_{ij}(I,R)\mid i\neq j\rangle,$$

当 R 为局部环时上式对一切 $I\subsetneqq R$ 成立。

定义 30.2　设 $R\in\mathfrak{R}\mathrm{ing}$，$I\lhd R$，记 $\mathrm{St}(R)$ 的子群

$$\mathrm{St}(I)=\langle x_{ij}(I)\mid i\neq j\rangle,$$
$$\mathrm{St}(R,I)=\mathrm{Ker}(\mathrm{St}(R)\to\mathrm{St}(R/I))=\mathrm{KerSt}(\pi),$$

其中 $\pi:R\twoheadrightarrow R/I$ 为标准环同态。

我们来证明

命题 30.2 设 $R\in \mathbb{R}\mathrm{ing}, I\lhd R$，则

(1) $\mathrm{St}(R,I)=\langle\{x\mathrm{St}(I)x^{-1}\mid x\in\mathrm{St}(R)\}\rangle\lhd \mathrm{St}(R)$；

(2) $\Xi(R,I)<\mathrm{St}(R,I)$，

$\mathrm{St}(I)<\mathrm{St}(R,I)$；

(3) $\Xi(R,I)\langle\{h\in\mathrm{St}(R)\mid h\mathrm{St}(I)h^{-1}=\mathrm{St}(I)\}\rangle\equiv N_{\mathrm{St}(R)}(\mathrm{St}(I))$（$\mathrm{St}(I)$在 $\mathrm{St}(R)$中的正规化子）；

(4) $\mathrm{St}(I)\Xi(R,I)=\Xi(R,I)\mathrm{St}(I)<\mathrm{St}(R,I)$。

证 (1) 由 $\mathrm{St}(R,I)$的定义知$\langle\{x\mathrm{St}(I)x^{-1}\mid x\in\mathrm{St}(R)\}\rangle\subseteq\mathrm{St}(R,I)$。

另一方面，$\forall y\in\mathrm{St}(R,I)$，$y$ 可表为

$$y=x_{i_1j_1}(a_1)x_{i_2j_2}(a_2)\cdots x_{i_kj_k}(a_k)$$

于是

$$\mathrm{St}(\pi)(y)=x_{i_1j_1}(\bar{a}_1)x_{i_2j_2}(\bar{a}_2)\cdots x_{i_kj_k}(\bar{a}_k)=1,$$

其中 $\bar{a}_l=\pi(a_l)$。注意 $\mathrm{St}(\pi)(y)=\mathrm{St}(\pi)(wyw^{-1})$，$\forall w\in \mathrm{W}(R)$，可得

$$\mathrm{St}(\pi)(wyw^{-1})=x_{i_1j_1}(\bar{0})$$

于是必有 $a\in I$ 使

$$wyw^{-1}=x_{i_1j_1}(a)$$

由此知

$$y=w^{-1}x_{i_1j_1}(a)w\in\langle\{x\mathrm{St}(I)x^{-1}\mid x\in\mathrm{St}(R)\}\rangle$$

这就证出了(1)。

(2) 显然有 $\mathrm{St}(I)<\mathrm{St}(R,I)$。下证$\Xi(R,I)<\mathrm{St}(R,I)$。事实上，$\forall H_{ij}(a,b)\in\Xi(R,I)$，其中 $a\in I$。记 $\alpha=1+ab,\beta=1+ba$，则

$$\begin{aligned}\mathrm{St}(\pi)(H_{ij}(a,b))&=x_{ji}(-\overline{b\alpha^{-1}})x_{ij}(\bar{a})x_{ji}(\bar{b})x_{ij}(-\overline{a\beta^{-1}})\\&\xlongequal[a\in I]{}x_{ji}(-\overline{b\alpha^{-1}})x_{ji}(\bar{b})\\&=x_{ji}(\overline{b(1-\alpha^{-1})})=x_{ji}(\overline{b(1-(1-a\beta^{-1}b))})\\&=x_{ji}(\overline{ba\beta^{-1}b})=x_{ji}(\bar{0})=1\end{aligned}$$

因此(2)成立。

(3) 由上节命题 29.1 知，$\forall h\in\Xi(R,I)$都是对角元，因此为单项元，于是

$$h\mathrm{St}(I)h^{-1}\subseteq\mathrm{St}(I),$$
$$h^{-1}\mathrm{St}(I)h\subseteq\mathrm{St}(I),\qquad\forall h\in\Xi(R,I)$$

由此即知

$$h\mathrm{St}(I)h^{-1}=\mathrm{St}(I),\qquad\forall h\in\Xi(R,I)$$

这又证出了(3)。

(4) 由(2)，(3)知，$\mathrm{St}(R,I)$的子群 $\mathrm{St}(I)$与$\mathscr{E}(R,I)$满足

$$\mathrm{St}(I)\,\mathscr{E}(R,I)=\mathscr{E}(R,I)\mathrm{St}(I)$$

因此(4)成立。 □

加一个条件“$I\subseteq J(R)$”可将上命题的(4)变成等式。即

命题 30.3　设 $R\in\mathscr{R}\mathrm{ing}, I\lhd R$ 且 $I\subseteq J(R)$，则

$$\mathrm{St}(R,I)=\mathrm{St}(I)\,\mathscr{E}(R,I)=\mathscr{E}(R,I)\mathrm{St}(I)$$

因此 $\mathrm{St}(I)\lhd \mathrm{St}(R,I)$且

$$\mathscr{E}(R,I)\simeq \mathrm{St}(R,I)/\mathrm{St}(I)。$$

证　由命题 30.2(4)已得

$$\mathrm{St}(R,I)\supseteq \mathrm{St}(I)\,\mathscr{E}(R,I)=\mathscr{E}(R,I)\mathrm{St}(I)$$

再来证明其反向包含关系。由命题 30.2(1)知，只需证

$$x_{ij}(a)\mathrm{St}(I)x_{ij}(a)^{-1}\subseteq \mathrm{St}(I)\,\mathscr{E}(R,I),\ \forall a\in R, i\neq j \tag{1}$$

事实上，$\forall b\in I$，由 $I\subseteq J(R)$知 $\alpha=1+ab, \beta=1+ba\in R^{\cdot}$。于是由 Steinberg 关系

$$x_{ij}(a)x_{kl}(b)x_{ij}(a)^{-1}=\begin{cases}x_{kl}(b), & k\neq j, l\neq i\text{ 时}\\ x_{il}(ab)x_{jl}(b), & k=j, l\neq i\text{ 时}\\ x_{kj}(-ba)x_{ki}(b), & k\neq j, l=i\text{ 时}\end{cases}$$

并注意

$$x_{ij}(a)x_{ji}(b)x_{ij}(a)^{-1}=x_{ji}(b\alpha^{-1})H_{ij}(a,b)x_{ij}(a\beta^{-1}-a),$$

$$\left.\begin{array}{l}a\beta^{-1}-a=a(\beta^{-1}-1)\\ \beta^{-1}=1-b\alpha^{-1}a\end{array}\right\}\Rightarrow\beta^{-1}-1\in I\Rightarrow a\beta^{-1}-a\in I,$$

$$b\alpha^{-1}\in I,$$

即得(1)。

这样，就证出了

$$\mathrm{St}(R,I)=\mathrm{St}(I)\,\mathscr{E}(R,I)=\mathscr{E}(R,I)\mathrm{St}(I) \tag{2}$$

又由命题 30.2(3)知

$$\mathscr{E}(R,I)\subseteq N_{\mathrm{St}(R)}(\mathrm{St}(I))$$

而 $\mathrm{St}(I)\subseteq N_{\mathrm{St}(R)}(\mathrm{St}(I))$是显见的。因此由(2)知

$$\mathrm{St}(I)\lhd \mathrm{St}(R,I),$$

$$\mathrm{St}(R,I)/\mathrm{St}(I)\simeq \mathscr{E}(R,I)。$$

□

仿照§10，§26 中 $T(R)$，$T'(R)$的定义再给出

定义 30.3　设 $R\in\mathscr{R}\mathrm{ing}$，记

$$T(I) = T(R) \cap \mathrm{St}(I) = \langle \{x_{ij}(a) \mid i < j, a \in I\} \rangle,$$
$$T'(I) = T'(R) \cap \mathrm{St}(I) = \langle \{x_{ij}(a) \mid i > j, a \in I\} \rangle。$$

注意到 $\forall h \in \mathbb{H}(R,I)$ 都是对角元，对应着恒等置换（见命题 26.1），用 $\mathbb{H}(R,I)$ 的定义立得

命题 30.4 设 $R \in \mathbb{R}\mathrm{ing}, I \lhd R$，则

(1) $\mathbb{H}(R,I) \subseteq N_{\mathrm{St}(R)}(T(I)) \equiv \{h \in \mathrm{St}(R) \mid hT(I)h^{-1} = T(I)\}$，$\mathbb{H}(R,I) \subseteq N_{\mathrm{St}(R)}(T'(I))$；

(2) $T'(I)T(I)\mathbb{H}(R,I) \subseteq \mathrm{St}(R,I)$。

加条件"$I \subseteq J(R)$"可将上命题中的(2)改为等式。即

命题 30.5 设 $R \in \mathbb{R}\mathrm{ing}, I \lhd R$ 且 $I \subseteq J(R)$。则

$$\mathrm{St}(R,I) = T'(I)T(I)\,\mathbb{H}(R,I)$$

证 由上命题(2)知，只需证

$$\mathrm{St}(R,I) \subseteq T'(I)T(I)\,\mathbb{H}(R,I)$$

记右端为 X，且放大右端，记 $Y = T'(R)T(I)\mathbb{H}(R,I)$，则 $X \subseteq Y$。

由 $\mathrm{St}(I)$ 的生成系 $\{x_{ij}(a) \mid i \neq j, a \in I\} \subseteq T'(I)T(I)$（注意不能由此断言 $\mathrm{St}(I) \subseteq T'(I)T(I)$！）与命题 30.3 中的 $\mathrm{St}(R,I) = \mathrm{St}(I)\mathbb{H}(R,I) = \mathbb{H}(R,I)\mathrm{St}(I)$，可知 $\{\mathrm{St}(R,I)$ 的生成系$\} \subseteq X \subseteq Y$。

下面先证

(1) $\mathrm{St}(R,I) \subseteq Y$。

为证(1)，只需证 $Y \cdot \{\mathrm{St}(R,I)$ 的生成系$\} \subseteq Y$，即证

$$YT'(R) \subseteq Y \tag{3}$$
$$YT(I) \subseteq Y \tag{4}$$

（注意由 Y 的定义，$Y\mathbb{H}(R,I) \subseteq Y$ 是显见的，因为 $\mathbb{H}(R,I)$ 为群，从而对乘法封闭）。事实上，由

$$[x_{i,i-1}(a), x_{i-1,i-r}(1)] = x_{i,i-r}(a), \quad \forall i > r \geqslant 2, a \in R$$

知

$$T'(R) = \langle \{x_{i,i-1}(a) \mid a \in R, i \geqslant 2\} \rangle$$

（注意 $1 \notin I$，不能由类似地方法得 $T'(I) = \langle \{x_{i,i-1}(a) \mid a \in I, i \geqslant 2\} \rangle$，因此上面用 $T'(R)$ 而不用 $T'(I)$）。任取 $t' \in T'(R), t \in T(I), h \in \mathbb{H}(R,I)$，若能证明

$$t'thx_{ij}(a) \in Y, \tag{5}$$

其中 $i<j$ 时 $a \in I$；$i>j$ 时（可令 $j=i-1$），$a \in R$ 即得(3)，(4)。

注意到 $T'(R)$，$\mathbb{H}(R,I)$ 都是群，由 Y 的定义知 $t'^{-1}Yh^{-1} = Y$。但 h 为对角元，对应着恒等置换，因此，可记

$$hx_{ij}(a)h^{-1}=x_{ij}(b)，当 a\in I 时 b\in I, a\in R 时当然 b\in R。$$

于是，如能证出

$$tx_{ij}(b)\in Y=t'^{-1}yh^{-1}, \forall b\in I, i<j 或 b\in R, j=i-1 \qquad (6)$$

则(5)即证出。

由命题 10.3 之证可类似地看出

$$T(I)=\langle\{C_r(\alpha)=x_{1r}(a_1)x_{2r}(a_2)\cdots x_{r-1,r}(a_{r-1})\mid r\geqslant 2,$$
$$\alpha=(a_1,\cdots,a_{r-1})\in I^{r-1}\}\rangle$$

分三种情况来证(6)。

(A) $r<i$ 时，显然有

$$C_r(\alpha)x_{i,i-1}(b)=x_{i,i-1}(b)C_r(\alpha)$$

(B) $r>i$ 时，

$$C_r(\alpha)x_{i,i-1}(b)=x_{i,i-1}(b)x_{1r}(a_1)\cdots x_{i-1,r}(a_{i-1})x_{ir}(a_i-ba_{i-1})\cdots$$
$$\cdots x_{r-1,r}(a_{r-1})$$
$$=x_{i,i-1}(b)C_r(\alpha'), \ \alpha'\in I^{r-1}$$

(C) $r=i$ 时，

$$C_i(\alpha)x_{i,i-1}(b)=x_{1i}(a_1)\cdots x_{i-2,i}(a_{i-2})x_{i-1,i}(a_{i-1})x_{i,i-1}(b)$$
$$=x_{1i}(a_1)\cdots x_{i-2,i}(a_{i-2})x_{i,i-1}(b\alpha_1^{-1})H_{i-1,i}(a_{i-1},b)x_{i-1,i}(a_{i-1}\beta_1^{-1})$$

(其中 $\alpha_1=1+a_{i-1}b, \beta_1=1+ba_{i-1}$)

$$=x_{i,i-1}(b\alpha_1^{-1})(x_{1i}(a_1)x_{1,i-1}(a_1b\alpha_1^{-1})\cdots(x_{i-2,i}(a_{i-2})x_{i-2,i-1}$$
$$(a_{i-2}b\alpha_1^{-1}))x_{i-1,i}(\alpha_1a_{i-1})H_{i-1,i}(a_{i-1},b)$$
$$=x_{i,i-1}(b\alpha_1^{-1})C_{i-1}(\alpha'')C_i(\alpha')H_{i-1,i}(a_{i-1},b)$$

(其中 $\alpha''\in I^{i-2}, \alpha'\in I^{i-1}$)。

由(A)，(B)，(C)知

$$tx_{i,i-1}(b)=x_{i,i-1}(b')t_0$$

其中 $b'\in R, t_0\in T(I)\Xi(R,I)$，由此知 $tx_{i,i-1}(b)\in Y, \forall b\in R$。在 $i<j, b\in I$ 时，由于 $x_{ij}(b)\in T(I)$，因此

$$tx_{ij}(b)\in T(I)\subseteq Y$$

这就证出了 $\mathrm{St}(R,I)\subseteq Y$。

(2) 由 $\mathrm{St}(R,I)\subseteq Y$ 知，$\forall u\in \mathrm{St}(R,I)$，$u$ 可表为

$$u=t'th, \ t'\in T'(R), \ t\in T(I), h\in \Xi(R,I)$$

由于 $T(I)$，$\Xi(R,I)$ 都是 $\mathrm{St}(R,I)$ 的子群，因此

$$t'=uh^{-1}t^{-1}\in \mathrm{St}(R,I)\cap T'(R)$$
$$=\mathrm{Ker}(T'(R)\to T'(R/I))=T'(I)$$

由此即知 $u\in X$，即 $\mathrm{St}(R,I)\subseteq T'(I)T(I)\mathbb{H}(R,I)$，从而命题证毕。 □

作为上命题的应用，我们给出如下的推论。

推论 30.1 设 $R\in\mathbb{R}\mathrm{ing}$，$I\lhd R$ 且 $I\subseteq J(R)$，$\pi:R\twoheadrightarrow R/I$ 为标准环同态，则

$$\mathrm{Ker}(\mathrm{K}_2\pi)\subseteq\mathbb{H}(R,I),$$

$$\mathrm{Ker}(\mathrm{K}_2\pi)=\mathrm{K}_2R\cap\mathbb{H}(R,I)。$$

证 容易看出 $\mathrm{Ker}(\mathrm{K}_2\pi)=\mathrm{K}_2R\cap\mathrm{St}(R,I)$，因此由上命题知，$\forall u\in\mathrm{Ker}(\mathrm{K}_2\pi)$，$u$ 必可表为

$$u=t'th,\ t'\in T'(I),\ t\in T(I),\ h\in\mathbb{H}(R,I)$$

由 $u\in\mathrm{K}_2R$ 知

$$1=\phi(u)=\phi(t')\phi(t)\phi(h),$$

其中 $\phi:\mathrm{St}(R)\to E(R)$ 为 Steinberg 同态。于是

$$\phi(t')^{-1}=\phi(t)\phi(h)$$

注意此式左边为下三角矩阵(对角元都是 1)；右边为上三角矩阵(对角元都是 1)与对角矩阵之积，因此是上三角矩阵，于是上式两端三矩阵都是对角矩阵，但此三矩阵又都是初等矩阵($\mathrm{E}(R)$中元素)。所以有

$$\phi(t')=\phi(t)=\phi(h)=1$$

由此知

$$t\in T(R)\cap\mathrm{K}_2R\overset{}{\underset{\text{命题 }10.3}{=\!=\!=}}1$$

即 $t=1$。同理知 $t'=1$。因此 $u=h\in\mathbb{H}(R,I)$，$\forall u\in\mathrm{Ker}(\mathrm{K}_2\pi)$，即

$$\mathrm{Ker}(\mathrm{K}_2\pi)\subseteq\mathbb{H}(R,I)$$

于是 $\mathrm{Ker}(\mathrm{K}_2\pi)\subseteq\mathrm{K}_2R\cap\mathbb{H}(R,I)\subseteq\mathrm{K}_2R\cap\mathrm{St}(R,I)=\mathrm{Ker}(\mathrm{K}_2\pi)$，故 $\mathrm{Ker}(\mathrm{K}_2\pi)=\mathrm{K}_2R\cap\mathbb{H}(R,I)$。 □

推论 30.2 设 $R\in\mathbb{R}\mathrm{ing}$，$I\lhd R$ 且 $I\subseteq J(R)$，记 $S=R/I$，则当 $\mathrm{K}_2S\subseteq\mathbb{H}(S)$ 时，$\mathrm{K}_2R\subseteq\mathbb{H}(R)$。

证 对标准环同态 $\pi:R\twoheadrightarrow R/I$，显然有群的满同态

$$\mathrm{St}(\pi):\mathrm{St}(R)\twoheadrightarrow\mathrm{St}(S)$$

先证 π 诱导出群的满同态

$$\mathbb{H}(\pi):\mathbb{H}(R)\twoheadrightarrow\mathbb{H}(S)$$

事实上，$\forall x,y\in S$，若 $1+xy\in S^{\cdot}$，则由 π 的满性知必有 $a,b\in R$ 使 $\pi(a)=x$，$\pi(b)=y$，$\pi(1+ab)=1+xy\in S^{\cdot}$，但 $1+xy=\delta+I$，$\delta\in R^{\cdot}$，又

$$\mathrm{Ker}\pi=I\subseteq J(R),$$

$$1+ab\in\delta+I,$$

因此 $1+ab\in R^{\cdot}$，即

$$\Xi(\pi)(H_{ij}(a,b)) = H_{ij}(x,y)$$

由此即知 $\Xi(\pi)$ 是满的。

再证 $K_2R\subseteq\Xi(R)$。任取 $u\in K_2R$，则

$$K_2(\pi)(u) = \bar{u} \in K_2S \subseteq \Xi(S)$$

由上段所证 $\Xi(\pi)$ 的满性知，必有 $h_1\in\Xi(R)$ 使 $\Xi(\pi)(h_1)=\bar{u}$。注意 $\mathrm{St}(\pi)|_{\Xi(R)}=\Xi(\pi)$，又知 $\mathrm{St}(\pi)(u)=\mathrm{St}(\pi)(h_1)$。因此

$$uh_1^{-1} \in \mathrm{St}(R,I) = \mathrm{Ker}(\mathrm{St}(\pi))$$

于是由上命题知，有 $t'\in T'(I)$，$t\in T(I)$ 与 $h\in\Xi(R,I)$ 使

$$uh_1^{1} = t'th$$

即 $u=t't(hh_1)$，其中 $hh_1\in\Xi(R,I)\Xi(R)=\Xi(R)$，因此为对角元。

由 $u\in K_2R$ 知，$\phi(u)=\phi(t'thh_1)=1$，用上推论后半段证法即得 $t=1$，$t'=1$。因此 $u=hh_1\in\Xi(R)$。这就证出了 $K_2R\subseteq\Xi(R)$。 □

用上推论于局部环，则得

推论 30.3　设 R 为局部环(未必为交换环)，则 $K_2R\subseteq\Xi(R)$。

证　由 R 为局部环(非可逆元对加法封闭)知 $S=R/J(R)$ 为除环。由上推论知，只需证 $K_2S\subseteq\Xi(S)$。

事实上，由命题 26.4 知，对除环 S，

$$K_2S = C(S) = \langle\{\{u,v\} \mid uv = vu, u,v \in S^{\cdot}\}\rangle$$

又由引理 26.2 知 $C(S)\subseteq H(S)$。另一方面，$\forall u\in S^{\cdot}$ 由推论 29.1 知 $\langle u-1,1\rangle=1$，而 $\langle a,b\rangle=H_{ij}(a,b)h_{ij}(\alpha)^{-1}$，$\alpha=1+ab$，$1+(u-1)\cdot 1=u$。于是

$$h_{ij}(u) = H_{ij}(u-1,1) \in \Xi(S)$$

由此知 $H(S)\subseteq\Xi(S)$。故

$$K_2S = C(S) \subseteq H(S) \subseteq \Xi(S)$$ □

由§26，我们已经知道，对 $R\in\mathscr{R}$ing，

$$C(R) = K_2R \cap W(R) \subseteq H(R) \subseteq W(R)$$

因此

$$C(R) = K_2R \cap H(R)$$

对 R 的理想 I 可给出更广义的

定义 30.4　设 $R\in\mathscr{R}$ing，$I\lhd R$，定义 $\mathrm{St}(R)$ 的下述子群：

$H(R,I) = \langle\{h_{ij}(u) \mid i\neq j, u\in R^{\cdot}$ 且 $u\equiv 1(\mathrm{mod}\ I)\}\rangle$，

$C(R,I) = K_2R \cap H(R,I)$，

$H(R) = H(R,R)$，

$C(R) = C(R,R)$。

容易看出 $\mathrm{H}(R)$,$\mathrm{C}(R)$与§26 的定义是一致的,且可证 $\mathrm{H}(R,I)\lhd \mathbb{H}(R,I)$。另一方面,容易直接验证如下结果:

命题 30.6 设 $R\in \mathbb{R}\mathrm{ing}$,$I\lhd R$,则

(1) $\mathrm{C}(R,I)=\mathrm{H}(R,I)\cap \mathrm{Ker}(\mathrm{K}_2(\pi))$,其中 $\pi:R\twoheadrightarrow R/I$ 为标准环同态;

(2) $\mathrm{C}(R,I)\subseteq \mathrm{C}(R)\cap \mathrm{St}(R,I)$;

$\mathrm{H}(R,I)\subseteq \mathrm{H}(R)\cap \mathrm{St}(R,I)$。

注① 一般地(见下例),上命题(2)中两式不是等式,即

$$\mathrm{C}(R,I)\subsetneqq \mathrm{C}(R)\cap \mathrm{St}(R,I)$$
$$\mathrm{H}(R,I)\subsetneqq \mathrm{H}(R)\cap \mathrm{St}(R,I)$$

例 1 设 $R=\mathbb{Z}$,$I=3\mathbb{Z}$,$S=R/I=\mathbb{Z}_3$,此时 $\mathrm{K}_2(S)=1$。

$$\{-1,-1\}\in \mathrm{C}(\mathbb{Z})\cap \mathrm{St}(\mathbb{Z},3\mathbb{Z})\subseteq \mathrm{H}(\mathbb{Z})\cap \mathrm{St}(\mathbb{Z},3\mathbb{Z})$$

但

$$\{u\in \mathbb{Z}^{\cdot}\mid u\equiv 1(\mathrm{mod}\ 3\mathbb{Z})\}=1$$

因此

$$\mathrm{C}(\mathbb{Z},3\mathbb{Z})=\mathrm{H}(\mathbb{Z},3\mathbb{Z})=1$$

下节中我们将证明:在 $\mathrm{K}_2\mathbb{Z}$(因此在 $\mathrm{St}(\mathbb{Z})$中$\{-1,-1\}\neq 1$。因此上命题中的(2)不能改进为等式。读者可去研究:对什么样的理想 I,它们成为等式?

仿照引理 26.2 与命题 26.2 的证法又可得

命题 30.7 设 $R\in \mathbb{R}\mathrm{ing}$,$I\lhd R$,则

(1) $\mathrm{H}(R,I)=\langle\{h_{1i}(u)\mid i\neq 1,u\in R^{\cdot}$ 且 $u\equiv 1(\mathrm{mod}\ I)\}\rangle$;

(2) 当 $R\in \mathbb{C}\mathrm{Ring}$ 时,

$$\mathrm{C}(R,I)=\langle\{\{u,v\}\mid u,v\in R^{\cdot}\text{ 且 }u,v\equiv 1(\mathrm{mod}\ I)\}\rangle。$$

仿照定义 30.4 又可给出如下定义。

定义 30.5 设 $R\in \mathbb{R}\mathrm{ing}$,$I\lhd R$,定义 $\mathrm{St}(R)$的下述子群

$$\mathbb{C}(R,I)=\mathrm{K}_2R\cap \mathbb{H}(R,I),$$
$$\mathbb{C}(R)=\mathbb{C}(R,R)。$$

由此定义与推论 30.1 立得

推论 30.1′ 设 $R\in \mathbb{R}\mathrm{ing}$,$I\lhd R$ 且 $I\subseteq J(R)$,$\pi:R\twoheadrightarrow R/I$ 为标准环同态,则

$$\mathrm{Ker}(\mathrm{K}_2\pi)=\mathbb{C}(R,I)$$

注意到由上定义知

$$\mathbb{C}(R)=\mathbb{H}(R)\cap \mathrm{K}_2R\subseteq \mathrm{K}_2R$$

于是由推论 30.2 又得（注意下面的条件 $K_2S\subseteq \mathbb{C}(S)$ 等价于 $K_2S=\mathbb{C}(S)$，因为 $\mathbb{C}(S)\subseteq K_2S$）。

推论 30.2′　设 $R\in \mathbb{R}\mathrm{ing}$，$I\lhd R$ 且 $I\subseteq J(R)$，记 $S=R/I$，则当 $K_2S\subseteq \mathbb{C}(S)$ 时 $K_2R=\mathbb{C}(R)$。

由此结果与推论 30.3 立得

定理 30.1　设 R 为局部环，则 $K_2R=\mathbb{C}(R)$。

对交换的局部环，我们将得到更好的结果，为此先考察 $\mathbb{C}(R,I)$ 的生成系，即证

命题 30.8　设 $R\in \mathbb{R}\mathrm{ing}$，$I\lhd R$，则

$$\mathbb{C}(R,I)=\langle\{\langle a,b\rangle \mid a,b\in R \text{ 且 } 1+ab\in R^{\cdot}, a\in I\}\rangle$$

证　(1) 先证 $\langle\{\langle a,b\rangle\mid a,b\in R \text{ 且 } 1+ab\in R^{\cdot}, a\in I\}\rangle\subseteq \mathbb{C}(R,I)$。令 $a,b\in R$，$\alpha=1+ab\in R^{\cdot}$，$a\in I$，则

$$H_{12}(a,b)\in \mathbb{H}(R,I)$$

$$h_{12}(\alpha)=H_{12}(\alpha-1,1)\text{（推论 29.1）}$$

$$\alpha-1=ab\in I$$

因此

$$h_{12}(\alpha)\in \mathbb{H}(R,I)$$

由此知（注意，由命题 29.3 知 $\langle a,b\rangle$ 的定义中可取 $i=1,j=2$）

$$\langle a,b\rangle=H_{12}(a,b)h_{12}(\alpha)^{-1}\in \mathbb{H}(R,I)\cap K_2R=\mathbb{C}(R,I)$$

(2) 再证 $\mathbb{C}(R,I)\subseteq\langle\{\langle a,b\rangle\mid a,b\in R \text{ 且 } 1+ab\in R^{\cdot}, a\in I\}\rangle$。

在 $H_{ij}(a,b)=\langle a,b\rangle h_{ij}(\alpha)$（其中 $\alpha=1+ab$）中 $\langle a,b\rangle\in K_2R=C(\mathrm{St}(R))$，因此 $\forall w\in \mathbb{C}(R,I)=K_2R\cap \mathbb{H}(R,I)$，W 可表为 $W=uh$，其中

$$u=\prod_{<\infty}\langle a_i,b_i\rangle,\ a_i\in I,\ h\in \mathrm{H}(R,I)$$

于是

$$h=wu^{-1}\in K_2R\cap \mathrm{H}(R,I)=\mathrm{C}(R,I)$$

但由命题 30.7(2)知，h 可表为

$$h=\prod_{<\infty}\{\alpha_j,\beta_j\},\alpha_j,\beta_j\in R^{\cdot} \text{ 且 } \alpha_j,\beta_j\equiv 1(\mathrm{mod}\ I)$$

记 $a_j'=(\alpha_j-1)\beta_j^{-1}$，则 $1+a_j'\beta_j=\alpha_j$，$a_j'\in I$。又由命题 29.5，注意 $\beta_j\in R^{\cdot}$，得

$$\{\alpha_j,\beta_j\}=\langle a_j',\beta_j\rangle,\ \forall j$$

$$1+a_j'\beta_j=\alpha_j\in R^{\cdot}$$

由此知 $h\in\langle\{\langle a,b\rangle\mid a,b\in R \text{ 且 } 1+ab\in R^{\cdot}, a\in I\}\rangle$，故由 $w=uh$ 知，(2)中欲证的包含关系成立。　□

由此命题与推论 30.1′,并注意 $1+J(R)\subseteq R^{\cdot}$,立得

推论 30.4 设 $R\in\mathcal{C}\mathrm{Ring}$,$I\lhd R$ 且 $I\subseteq J(R)$,记 $\pi:R\twoheadrightarrow R/I$ 为标准环同态,则

$$\mathrm{Ker}(\mathrm{K}_2\pi)=\langle\{\langle a,b\rangle\mid a,b\in R,a\in I\}\rangle$$

推论 30.5 设 $R\in\mathcal{C}\mathrm{Ring}$,$I\lhd R$ 且 $I\subseteq J(R)$,$S=R/I$,同时

$$\mathrm{K}_2S=\langle\{\{u,v\}\mid u,v\in S^{\cdot}\}\rangle$$

或

$$\mathrm{K}_2S=\langle\{\langle a',b'\rangle\mid a',b'\in S \quad 且 \quad 1+a'b'\in S^{\cdot}\}\rangle,$$

则

$$\mathrm{K}_2R=\langle\{\langle a,b\rangle\mid a,b\in R\ 且\ 1+ab\in R^{\cdot}\}\rangle。$$

证 由命题 29.5 知对 $u,v\in R^{\cdot}$,$1+(u-1)v^{-1}v=u$,因此

$$\{u,v\}=\langle(u-1)v^{-1},\ v\rangle$$

于是 $\mathrm{K}_2S=\langle\{\{u,v\}\mid u,v\in S^{\cdot}\}\rangle$ 时,$\mathrm{K}_2S\subseteq\langle\{\langle a',b'\rangle\mid a',b'\in S$ 且 $1+a'b'\in S^{\cdot}\}\rangle$,即 $\mathrm{K}_2S=\langle\{\langle a',b'\rangle\mid a',b'\in S$ 且 $1+a'b'\in S^{\cdot}\}\rangle$(注意 $\langle a',b'\rangle\in\mathrm{K}_2S$)。这又等价于 $\mathrm{K}_2S=\mathcal{C}(S)$(用命题 30.8,令 $I=R$)。故由推论 30.2′ 知 $\mathrm{K}_2R=\mathcal{C}(R)$,即 $\mathrm{K}_2R=\langle\{\langle a,b\rangle\mid a,b\in R$ 且 $1+ab\in R^{\cdot}\}\rangle$。 □

由此命题又可以得到

推论 30.6 设 $R\in\mathcal{C}\mathrm{Ring}$,则

$$\mathcal{C}(R)=\langle\{\langle a,b\rangle\mid a,b\in R\ 且\ 1+ab\in R^{\cdot}\}\rangle。$$

于是由定理 30.1 与此推论又得

定理 30.2 设 R 为交换局部环,则

$$\mathrm{K}_2R=\mathcal{C}(R)=\langle\{\langle a,b\rangle\mid a,b\in R\ 且\ 1+ab\in R^{\cdot}\}\rangle。$$

注② 记

$$c_i(u,v)=[h_{ij}(u),h_{ik}(v)],\ \forall\, u,v\in R^{\cdot},i\neq j,k,$$

$$b_1(1)=1,b_1(\alpha)\in \mathrm{H}(R),\ \forall\,\alpha\in R^{\cdot\prime}=[R^{\cdot},R^{\cdot}]\ 使$$

$$\varphi(b_1(\alpha))=a_1(\alpha)=\mathrm{diag}(\alpha,1,1,\cdots),$$

$$a_i(u)=\mathrm{diag}(1,\cdots,1,u,1,1,\cdots),\ \forall\, u\in R^{\cdot},$$

$$b_i(\alpha)=w_{1i}(-1)b_1(\alpha)w_{1i}(-1)^{-1},\ \forall\, i\neq 1,\alpha\in R^{\cdot\prime},$$

$$d(\alpha,\beta)=b_1(\alpha)b_1(\beta)b_1(\alpha\beta)^{-1},\ \forall\,\alpha,\beta\in R^{\cdot\prime},$$

$$e(u,v)=c_1(u,v)b_1([u,v])^{-1},\ \forall\, u,v\in R^{\cdot}。$$

注意 $c_1(\alpha,\beta)\in\mathrm{H}(R)$,$\forall\,\alpha,\beta\in R^{\cdot\prime}$,$a_i(\alpha)a_i(\beta)a_i(\alpha\beta)^{-1}=1$,$\forall\,\alpha,\beta\in R^{\cdot\prime}$,知 $\phi(d(\alpha,\beta))=1$,因此 $d(\alpha,\beta)\in\mathrm{K}_2R$,且当 $uv=vu$ 时 $e(u,v)=\{u,v\}$。

对于任意环 R,可证:$\mathrm{C}(R)=\langle\{e(u,v),d(\alpha,\beta)\mid u,v\in R^{\cdot},\alpha,\beta\in$

$R^{\cdot\,\prime}\}\rangle$;当 R 为半局部环时,$K_2R=C(R)$,但对 $K_2R=C(R)$成立的环找这些生成系的关系集十分困难。1976 年 S. M. Green 在[Green,1976]中对 R 为除环的情况进行尝试也未能成功。

满足 $K_2R\subseteq H(R)$的环 R 又称为 **H 环**(H-环),这等价于 $K_2R=C(R)$。比如除环,域,半局部环,局部环都是 H 环。对 H 环可证:有群正合列

$$1\to K_2R\to U_R\to R^{\cdot\,\prime}\to 1,$$

其中 $U_R=\langle C_1(R^{\cdot},R^{\cdot})\rangle$为 $St(R)$的子群。当 R 为除环时,可证其关系集为

$$c_1(\alpha,1-\alpha)=1,\forall\alpha\neq 0,1,$$
$$c_1(\alpha\beta,\gamma)=c_1(\alpha\beta\alpha^{-1},\alpha\gamma\alpha^{-1})c_1(\alpha,\gamma),$$
$$c_1(\alpha,\beta\gamma)c_1(\beta,\gamma\alpha)c_1(\gamma,\alpha\beta)=1。$$

显然,当 R 为交换 H 环时 $R^{\cdot\,\prime}=1$,因此,$K_2R\simeq U_R$。

§31 $\mathbb{Z}_n$ 与$\mathbb{Z}$ 的 K_2 群及相对 K_i 群的正合列

如众周知,当环 R 的特征数为 0 时,R 的最小子环同构于$\mathbb{Z}$;当环 R 的特征数为 n 时,R 的最小子环同构于$\mathbb{Z}_n\equiv\mathbb{Z}/n\mathbb{Z}$。因此$\mathbb{Z}_n$ 与$\mathbb{Z}$ 是两个重要的环,研究它们的 K_2 群是有意义的。又由于研究它们 K_2 群时用到的一些方法也是有用的方法之一,因此本节中我们专门研究这两个环的 K_2 群。

在命题 25.2 中我们已经得到下述结果:若 $4\nmid n$,则 $K_2\,\mathbb{Z}_n$ 中的子群 $\{\mathbb{Z}_n^{\cdot},\mathbb{Z}_n^{\cdot}\}=1$。下面对 $K_2\,\mathbb{Z}_n$ 我们将证明

$$K_2\,\mathbb{Z}_n=\begin{cases}\langle\{-1,-1\}\rangle\simeq\mathbb{Z}_2, & 4\mid n\text{ 时}\\ 1, & 4\nmid n\text{ 时}\end{cases}$$

首先注意,若记 n 的标准分解为

$$n=2^{a_0}p_1^{a_1}p_2^{a_2}\cdots p_m^{a_m},$$

其中 $p_1,p_2,\cdots,p_m$ 为互异的奇素数。于是$\mathbb{Z}_n$ 有环的分解式

$$\mathbb{Z}_n\simeq\mathbb{Z}_{2^{a_0}}\oplus\mathbb{Z}_{p_1^{a_1}}\oplus\mathbb{Z}_{p_2^{a_2}}\oplus\cdots\oplus\mathbb{Z}_{p_m^{a_m}}$$

因此有相应的 K_2 群直和分解式(用定理 10.3)。从而研究 $K_2\,\mathbb{Z}_n$ 归为研究 $K_2\,\mathbb{Z}_{p^r}$,而对素数 p,$\mathbb{Z}_{p^r}$ 都是交换局部环,其惟一极大理想为 $\mathfrak{m}=p\mathbb{Z}_{p^r}$。考察一系列的环的标准满同态

$$\mathbb{Z}_{p^{k+1}}\xrightarrow{f}\mathbb{Z}_{p^k}\twoheadrightarrow\mathbb{Z}_{p^{k-1}}\twoheadrightarrow\cdots\twoheadrightarrow\mathbb{Z}_p(\text{有限域}),$$

则得一系列的 K_2 群同态

$$K_2\,\mathbb{Z}_{p^{k+1}} \xrightarrow{K_2 f} K_2\,\mathbb{Z}_{p^k} \to K_2\,\mathbb{Z}_{p^{k-1}} \to \cdots \to K_2\,\mathbb{Z}_p = 1 \qquad (*)$$

由此知，确定 $\mathrm{Ker}(K_2 f)$是一个关键问题。对此，我们给出

命题 31.1 设 p 为素数，$k \geqslant 1$，且

$$f: \mathbb{Z}_{p^{k-1}} \twoheadrightarrow \mathbb{Z}_{p^k}$$

为标准环同态，则

(1) $|\mathrm{Ker}(K_2 f)| \begin{cases} =1, & p>2 \text{ 或 } k>1 \\ \leqslant 2, & p=2 \text{ 且 } k=1 \end{cases}$

(2) $p>2$ 或 $k>1$ 时，$K_2 f: K_2\,\mathbb{Z}_{p^{k-1}} \to K_2\,\mathbb{Z}_{p^k}$ 为群同构，因此

$$K_2\,\mathbb{Z}_{p^{k+1}} \simeq K_2\,\mathbb{Z}_{p^k} \simeq \cdots \simeq K_2\,\mathbb{Z}_{p^2}$$

证 注意 $\mathbb{Z}_{p^{k-1}}$ 为交换局部环，其惟一极大理想为 $\mathfrak{m} = p\mathbb{Z}_{p^{k+1}} = J(\mathbb{Z}_{p^{k+1}})$，而

$$\mathrm{Ker} f = p^k \mathbb{Z}_{p^{k+1}} \subseteq J(\mathbb{Z}_{p^{k-1}})$$

因此由推论 30.4 知

$$\mathrm{Ker}(K_2 f) = \langle \{\langle ap^k, b\rangle \mid a, b \in \mathbb{Z}\}\rangle$$

现在，分两步来证明

$$\mathrm{Ker}(K_2 f) = \langle\langle p^k, p^k\rangle\rangle$$

(A) $\langle cp^k, dp^k\rangle = \langle p^k, p^k\rangle^{cd}$，$\forall c, d \in \mathbb{Z}$。

事实上，注意在环$\mathbb{Z}_{p^{k+1}}$中 $p^{k+j} \equiv 0 \pmod{p^{k+1}}$，$\forall j \geqslant 1$。我们有

$$\begin{aligned}\langle cp^k, dp^k\rangle\langle cp^k, ep^k\rangle &= \langle cp^k, dp^k + ep^k + dcep^{3k}\rangle \\ &= \langle cp^k, (d+e)p^k\rangle, \quad \forall c, d, e \in \mathbb{Z}\end{aligned}$$

因此

$$\langle cp^k, dp^k\rangle = \langle cp^k, p^k\rangle^d$$

类似地，有

$$\langle -p^k, -cp^k\rangle = \langle -p^k, -p^k\rangle^c$$

于是

$$\langle cp^k, p^k\rangle = \langle -p^k, -cp^k\rangle^{-1} = \langle -p^k, -p^k\rangle^{-c} = \langle p^k, p^k\rangle^c$$

这就证出了(A)。

(B) 由

$$\begin{aligned}&\langle ap^k, b\rangle\langle ap^k, c\rangle = \langle ap^k, b + c + bacp^k\rangle \\ &= \langle ap^k, (b+c) + bacp^k + (b+c)a^2bcp^{2k}\rangle \\ &\qquad (\text{注意 } p^{2k} \equiv 0 \pmod{p^{k+1}}) \\ &= \langle ap^k, b+c\rangle\langle ap^k, abcp^k\rangle \xlongequal{(A)} \langle ap^k, b+c\rangle\langle p^k, p^k\rangle^{a^2bc} \\ &\equiv \langle ap^k, b+c\rangle \pmod{\langle p^k, p^k\rangle}\end{aligned}$$

知

$$\langle ap^k, b\rangle \equiv \langle ap^k, 1\rangle^b \pmod{\langle p^k, p^k\rangle}$$

再由 $\langle ap^k, 1\rangle^b = 1^b = 1$ 即知 $\mathrm{Ker}(K_2 f) = \langle\langle p^k, p^k\rangle\rangle$。

再设 $k>1$，在命题 29.6(3)中取 $a=p^k, b=p, c=p^{k-1}$，则有(注意 $p^k \cdot p^{k-1} \equiv p \cdot p^k \equiv 0 \pmod{p^{k+1}}$)

$$\langle p^k, p\cdot p^{k-1}\rangle\langle p, p^k\cdot p^{k-1}\rangle\langle p^{k-1}, p\cdot p^k\rangle = 1$$

由此知：当 $k>1$ 时 $\langle p^k, p^k\rangle = 1$，即 $\mathrm{Ker}(K_2 f) = 1$。

设 $k=1$，则由

$$\langle p,p\rangle\langle p,-p\rangle = \langle p, p-p-p^3\rangle = \langle p, -p^3\rangle = \langle p, 0\rangle = 1$$

知 $\langle p,-p\rangle = \langle p,p\rangle^{-1}$。又由 $\langle a,b\rangle = \langle -b,-a\rangle^{-1}$ 知

$$\langle p,-p\rangle = \langle p,-p\rangle^{-1}$$

于是 $\langle p,p\rangle$ 与 $\langle p,-p\rangle$ 的阶数为 1 或 2，由此知 $|\mathrm{Ker}(K_2 f)| \leqslant 2$。但

$$\langle p,p\rangle^p \xlongequal[\text{令 } c=1,\, d=p,\text{用}(A)]{} \langle p, p^2\rangle = \langle p, 0\rangle = 1$$

因此，若 $p>2$，则 $p=2l+1$，此时

$$1 = \langle p,p\rangle^p = \langle p,p\rangle^{2l+1} = \langle p,p\rangle$$

于是 $\mathrm{Ker}(K_2 f) = 1$。

这就证出了(1)。

再来证(2)。

设 $p>2$，由上段证明知(*)中的群同态都是单同态。因此

$$K_2\,\mathbb{Z}_{p^k} = 1, \qquad \forall k \geqslant 1$$

由此当然地有：$K_2 f$ 为群同构。

设 $p=2$，同理知，有单同态

$$K_2\,\mathbb{Z}_{2^k} \rightarrowtail K_2\,\mathbb{Z}_4, \qquad \forall k \geqslant 3$$

设 $p=2$ 且 $k=1$，记 $f: \mathbb{Z}_4 \twoheadrightarrow \mathbb{Z}_2$(有限域)，则有

$$K_2 f: K_2\,\mathbb{Z}_4 \to K_2\,\mathbb{Z}_2 = 1$$

因此 $\mathrm{Ker}(K_2 f) = K_2\,\mathbb{Z}_4$。但由上证已知 $|\mathrm{Ker}(K_2 f)| \leqslant 2$，再注意在 $\mathbb{Z}_4$ 中 $2=-2, 3=-1$，则知 $\langle 2,2\rangle = \langle 2,-2\rangle = \langle 2,1\rangle\langle 2,-1\rangle = \langle 2,-1\rangle$，于是

$$K_2\,\mathbb{Z}_4 = \langle\langle 2,-1\rangle\rangle$$

又由 $1+2(-1) = -1 \in \mathbb{Z}_{2^k}^*$ 知 $\langle 2,-1\rangle \in K_2\,\mathbb{Z}_{2^k}$，$\forall k \geqslant 2$，因此

$$K_2\,\mathbb{Z}_{2^k} = \langle\langle 2,-1\rangle\rangle, \langle 2,-1\rangle^2 = 1, \quad \forall k \geqslant 2$$

且当 $K_2\,\mathbb{Z}_4 = 1$ 时 $K_2 f$ 为同构，而当 $K_2\,\mathbb{Z}_4 \simeq \mathbb{Z}_2$，$k>1$ 时 $K_2 f$ 也是同构。由此知，$k>1$ 时 $K_2 f$ 必为同构。 □

由上证明顺便得到了定理 26.2(有限域的 K_2 群平凡)的下述推广。

推论 31.1 设 p 为奇素数，则

$$K_2\,\mathbb{Z}_{p^k} = 1, \qquad \forall k \geqslant 1$$

现在可证下述结果。

命题 31.2

$$K_2\,\mathbb{Z}_n \begin{cases} = 1, & 4 \nmid n, \\ \simeq 1 \text{ 或 } \mathbb{Z}_2, & 4 \mid n, \end{cases} \qquad \forall n > 1$$

证 令 n 的标准分解为

$n = 2^{a_0} p_1^{a_1} p_2^{a_2} \cdots p_m^{a_m}$，其中 $p_1, p_2, \cdots, p_m$ 为互异的奇素数。

由中国剩余定理(CRT)知

$$\mathbb{Z}_n \simeq \mathbb{Z}_{2^{a_0}} \oplus \mathbb{Z}_{p_1^{a_1}} \oplus \mathbb{Z}_{p_2^{a_2}} \oplus \cdots \oplus \mathbb{Z}_{p_m^{a_m}}$$

于是由定理 10.3 知

$$K_2\,\mathbb{Z}_n \simeq K_2\,\mathbb{Z}_{2^{a_0}} \oplus K_2\,\mathbb{Z}_{p_1^{a_1}} \oplus K_2\,\mathbb{Z}_{p_2^{a_2}} \oplus \cdots \oplus K_2\,\mathbb{Z}_{p_m^{a_m}}$$

由上命题之证知 $K_2\,\mathbb{Z}_{2^{a_0}} \simeq 1$，或 $\mathbb{Z}_2$，$K_2\,\mathbb{Z}_{p_j^{a_j}} = 1$，由此即得证。 □

命题 31.3 设 $n>1$，$\pi: \mathbb{Z} \twoheadrightarrow \mathbb{Z}_n$ 为标准环同态，则

$$K_2\pi: K_2\,\mathbb{Z} \to K_2\,\mathbb{Z}_n$$

为群的满同态。

证 由命题 31.1 之证知

$$K_2\,\mathbb{Z}_n = \langle\langle 2, -1\rangle\rangle \text{ 或 } 1$$

又由 $1+2(-1)=-1 \in \mathbb{Z}^{\cdot}$ 知 $\langle 2, -1\rangle \in K_2\mathbb{Z}$。因此 $K_2\pi$ 为满同态。

□

事实上，更一般地，有

推论 31.2 在 $K_2\,\mathbb{Z}, K_2\,\mathbb{Z}_n, K_2\,\mathbb{Q}, K_2\,\mathbb{R}, K_2\,\mathbb{C}, K_2F$ (F 为数域或 $\mathbb{C}$ 的子环)中

$$\langle 2, -1\rangle = \{-1, -1\}, \ \{-1, -1\}^2 = 1$$

证 记 $R=\mathbb{Z}, \mathbb{Z}_n, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ 或 F，总有 $1+2(-1)=-1\in R^{\cdot}$，因此用命题 29.5 即得证。 □

下面我们来证在 $\mathbb{Z}, \mathbb{Q}$ 等常见环的 K_2 群中，$\{-1,-1\}$(即 $\langle 2,-1\rangle$)都是 2 阶元(注意，可证，在 $K_2\,\mathbb{R}$ 中，$\mathrm{ord}\{-1,-1\}=2$，但在 $K_2\,\mathbb{C}$ 中，$\{-1,-1\}=\{i,-i\}^4=1$)。

命题 31.4 (1) 在 $K_2\,\mathbb{Q}$ 中 $\{-1,-1\}\neq 1$，即 $\mathrm{ord}\{-1,-1\}=\mathrm{ord}\langle 2, -1\rangle=2$；

(2) 若有环同态 $f: R \to S < \mathbb{Q}$，则在 K_2R 中(因此在 $K_2\,\mathbb{Z}$ 中)，$\mathrm{ord}\{-1, -1\}=\mathrm{ord}\langle 2,-1\rangle=2$；

(3) 记 $R=\{\frac{m}{n}\in\mathbb{Q}\mid 2\nmid n\}\equiv\mathbb{Z}_{(2)}$，则在 K_2R 中 $\mathrm{ord}\{-1,-1\}=\mathrm{ord}\langle 2,-1\rangle=2$。

证　(1) 用定义 27.1($p=2$ 时)中的表示法

$$-1=(-1)^1 2^0 5^0\frac{1}{1},\quad 即\ i=1,j=k=0$$

知，对 Steinberg 符号$(\ ,\ )_2$

$$(-1,-1)_2=(-1)^{u+jk+kj}=-1\in A_2=\{\pm 1\}$$

而$\mathbb{Q}$为域，因此$\{\ ,\ \}$为泛 Steinberg 符号，因此有群同态 $h:K_2\mathbb{Q}\to A_2$ 使 $h(\{-1,-1\})=(-1,-1)_2=-1$。由此即知$\{-1,-1\}\neq 1$(在 $K_2\mathbb{Q}$ 中)。但$\{-1,-1\}^2=\{1,-1\}=1$，$\{-1,-1\}=\langle 2,-1\rangle$，因此这又等价于 $\mathrm{ord}\{-1,-1\}=\mathrm{ord}\langle 2,-1\rangle=2$。

(2) 由(1)即得，(2)⇒(3)也是显见的。　□

下面再证在 $K_2\mathbb{Z}_8$ 中 $\mathrm{ord}\{-1,-1\}=2$。为此先证一条引理。

引理 31.1　设 R 为交换局部环，$I\overset{\triangleleft}{\neq}R$ 且 $\pi:R\twoheadrightarrow R/I$ 为标准环同态，则

$$\mathrm{Ker}(K_2\pi)=\langle\{\{u,v\}\mid u,v\in R^{\cdot}\ 且\ u\equiv 1\ (\mathrm{mod}\ I)\}\rangle$$

证　由推论 30.4(注意 $I\overset{\triangleleft}{\neq}R$ 时 $I\subseteq J(R)$，因为 R 为交换局部环)知

$$\mathrm{Ker}(K_2\pi)=\langle\{\langle a,b\rangle\mid a\in I,b\in R\}\rangle$$

若 $b\in R^{\cdot}$，则由命题 29.5 知，$\langle a,b\rangle=\{1+ab,b\}$。又显见 $1+ab\equiv 1\ (\mathrm{mod}\ I)$。

若 $b\notin R^{\cdot}$，则由 R 为局部环知，$a,b\in J(R)=\mathfrak{m}$ 且

$$\langle a,b\rangle\langle a,1\rangle=\langle a,1+b+ba\rangle$$

但 R 为局部环，$b+ba\in J(R)$，因此，$1+b+ba\in R^{\cdot}$。由此又知

$$\langle a,b\rangle=\langle a,1+b+ba\rangle=\{1+a(1+b+ba),1+b+ba\},$$

其中

$$1+a(1+b+ba)\equiv 1\ (\mathrm{mod}\ I)$$
$$1+b+ba\in R^{\cdot}$$
$$1+a(1+b+ba)\in R^{\cdot}$$

综上即得欲证。　□

命题 31.5　在 $K_2\mathbb{Z}_8$ 中 $\mathrm{ord}\{-1,-1\}=2$。

证　记 $R=\mathbb{Z}_{(2)}=\{\frac{m}{n}\in\mathbb{Q}\mid 2\nmid n\}$，则 R 为交换局部环且

$$R/8R\simeq\mathbb{Z}_{(2)}/8\,\mathbb{Z}_{(2)}\simeq\mathbb{Z}_8$$

为证此命题只需证$\{-1,-1\}\notin \mathrm{Ker}(K_2R\to K_2R/8R)$。

事实上，$\forall u\in 1+8R$，

$$u=1+\frac{8m}{n}$$
$$=\frac{n+8m}{n},2\nmid n$$

由 $2\nmid n$ 知 $n\equiv 1,3,5,7 \pmod 8$，因此(通过分子、分母同乘适当的数)可设 $n\equiv 1 \pmod 8$。于是

$$u=\frac{n+8m}{n}=(-1)^0 2^0 5^0\ \frac{n+8m}{n},\ n+8m,\ n\equiv 1 \pmod 8$$

由此可看出$(u,R^{\cdot})_2=1$，但由命题 31.4 之证已知$(-1,-1)_2=-1$。于是由上引理知，$\{-1,-1\}\notin \mathrm{Ker}(K_2R\to K_2R/8R)$，即在 $K_2\,\mathbb{Z}_8\simeq K_2R/8R$ 中$\{-1,-1\}\neq 1$，即 $\mathrm{ord}\{-1,-1\}=2$。 □

现在可以完全确定 $K_2\,\mathbb{Z}_n$ 如下。

定理 31.1

$$K_2\,\mathbb{Z}_n=\begin{cases}\langle\langle\{-1,-1\}\rangle\rangle\simeq\mathbb{Z}_2, & 4\mid n, \qquad (\text{R. K. Dennis})\\ 1, & 4\nmid n。\end{cases}$$

证 由命题 31.2 已知，当 $4\nmid n$ 时 $K_2\,\mathbb{Z}_n=1$，只需再考察 $4\mid n$ 的情况。又由命题 31.2 之证知，只需对 $n=2^k,k>1$，证明 $K_2\,\mathbb{Z}_{2^k}\simeq\mathbb{Z}_2$。

事实上，由推论 31.2 已知，此时$\langle 2,-1\rangle=\{-1,-1\}$。由命题 31.2 又知

$$K_2\,\mathbb{Z}_{2^k}\simeq 1\text{ 或 }\mathbb{Z}_2$$

又由命题 31.1 之证知

$$K_2\,\mathbb{Z}_{2^k}=\langle\langle 2,-1\rangle\rangle$$

且由命题 31.1 知

$$K_2\,\mathbb{Z}_{2^k}\simeq K_2\,\mathbb{Z}_{2^{k-1}}\simeq\cdots\simeq K_2\,\mathbb{Z}_8\simeq K_2\,\mathbb{Z}_4$$

但由命题 31.5 已知，在 $K_2\,\mathbb{Z}_8$ 中$\{-1,-1\}$为 2 阶元。于是

$$K_2\,\mathbb{Z}_{2^k}\simeq\mathbb{Z}_2,\qquad \forall k>1$$ □

下面来研究 $K_2\,\mathbb{Z}$，在命题 31.4 中已知 $\mathrm{ord}\{-1,-1\}=2$，因此$\mathbb{Z}_2<K_2\,\mathbb{Z}$。下面不用[Rosenberg,1994]中研究 $K_2\,\mathbb{Z}$ 的同调方法，来证明 $K_2\,\mathbb{Z}\simeq\mathbb{Z}_2$。先给出一个定义。

定义 31.1 设 $R\in\mathbb{R}\mathrm{ing}$，用定义 10.2 中的记号 $\mathrm{St}_n(R)$，并对 $R=\mathbb{Z}$ 使用如下记号：

$x_{ij}^1=x_{ij}=x_{ij}(1)$，$x_{ij}^{\lambda}=x_{ij}(\lambda)$，$\forall 1\leqslant i,j\leqslant n,i\neq j$，

$\alpha X=\alpha\phi(X)$(注意 $\phi(X)\in E_n(\mathbb{Z})$)，$\forall\alpha\in\mathbb{Z}^n=\mathbb{Z}^{1\times n}$，$X\in\mathrm{St}_n(\mathbb{Z})$，

$(a,b)x_{12}=(a,a+b)$，

$(a,b)x_{21}=(a+b,b)$，

$\|\alpha\|=|a_1|+|a_2|+\cdots+|a_n|,\ \forall\alpha=(a_1,a_2,\cdots,a_n)\in\mathbb{Z}^n$，

$\pm\beta\in\{(1,0,\cdots,0),\cdots,(0,0,\cdots,0,1)\}$（标准正交基，因此 $\|\pm\beta\|=1$），

$w_{ij}=w_{ij}(1)=x_{ij}x_{ji}^{-1}x_{ij},\ \forall 1\leqslant i,j\leqslant n,i\neq j$，

$W=W_n=W_n(\mathbb{Z})$。

先给出几个引理。

引理 31.2　设 $w\in W_n(\mathbb{Z}),\alpha\in\mathbb{Z}^n$，则

(1) $\|\alpha w\|=\|\alpha\|$；

(2) $w=w_{ij}(\pm1)$ 时，$\pm\beta w\in\{(1,0,\cdots,0),\cdots,(0,0,\cdots,0,1)\}$。

证　令 $w=w_{ij}(u)=x_{ij}(u)x_{ji}(-u^{-1})x_{ij}(u),u\in\mathbb{Z}^*$，即 $u=\pm1,\alpha=(a_1,a_2,\cdots,a_n)$，则

$$\begin{aligned}\alpha w&=(a_1,a_2,\cdots,a_n)e_{ij}^{u}e_{ji}^{-u^{-1}}e_{ij}^{u}\\&=(a_1,a_2,\cdots,a_i,\cdots,a_j+ua_i,\cdots,a_n)e_{ji}^{-u^{-1}}e_{ij}^{u}\\&=(a_1,a_2,\cdots,a_i-u^{-1}(a_j+ua_i),\cdots,a_j+ua_i,\cdots,a_n)e_{ij}^{u}\\&=(a_1,a_2,\cdots,-u^{-1}a_j,\cdots,ua_i,\cdots,a_n)\end{aligned}$$

注意 $u=\pm1$，即得 $\|\alpha w\|=\|\alpha\|$，即(1)成立。由此又显见(2)成立。□

引理 31.3(J. R. Silvester 引理)　设 $X\in St_n(\mathbb{Z}),n\geqslant2$，则 X 可表为 $X=g_1g_2\cdots g_mw$，其中 $w\in W_n,g_k\in\{x_{ij}^{\pm1}\mid i\neq j\}$，使

$$\|\beta g_1\|\leqslant\|\beta g_1g_2\|\leqslant\cdots\leqslant\|\beta g_1g_2\cdots g_m\|$$

证　记 $\sigma_0=1,\sigma_j=\|\beta g_1g_2\cdots g_j\|$，若欲证成立，即 $1\leqslant\sigma_1\leqslant\sigma_2\leqslant\cdots\leqslant\sigma_m$，则令 $\lambda=\mu=1$。否则，记

$$\lambda\equiv\max\{\sigma_j\mid\sigma_j>\sigma_{j+1}\},$$
$$\mu\equiv\max\{j\mid\sigma_j=\lambda>\sigma_{j+1}\}。$$

按字典序定义(λ,μ)的大小。只需证（注意 X 可表为 $X=g_1g_2\cdots g_mw$ 是显见的）：

$(\lambda,\mu)>(1,1)$ 时必可用 Steinberg 关系使(λ,μ) 严格减小（记为$(\lambda,\mu)\downarrow$）。

于是经有限步即可得证。

设$(\lambda,\mu)>(1,1)$（此时必 $\mu\geqslant1$，否则得 $1=\sigma_0>\sigma_1$，这不可能）。若 $g_\mu=x_{ij}$，则可经重编坐标的序号使$(i,j)\rightarrow(1,2)$。于是可设 $g_\mu=x_{12}$。若 $g_\mu=x_{ij}^{-1}$，注意以 βw_{ij}^{-1}代替 β（用引理 31.2），以 $w_{ij}w$ 作新的 w，则在

$$\beta X = \beta g_1 g_2 \cdots g_m w = (\beta w_{ij}^{-1})(w_{ij} g_1 w_{ij}^{-1}) \cdots (w_{ij} g_m w_{ij}^{-1})(w_{ij} w)$$

中，$g_\mu = x_{ij}^{-1}$ 变成 x_{ji}，因此，不失一般地可设 $g_\mu = x_{12}$，且

$$\beta g_1 \cdots g_\mu = (a, b, c, \cdots) \in \mathbb{Z}^n$$

$$\beta g_1 \cdots g_{\mu-1} = (a, b-a, c, \cdots) \in \mathbb{Z}^n$$

由此知"$\sigma_{\mu-1} \leqslant \sigma_\mu$"$\Leftrightarrow |b-a| \leqslant |b| \Leftrightarrow$

$$|a| \leqslant 2|b| \text{ 且 } a \neq 0 \text{ 时 } ab > 0。\qquad (*)$$

下面对 $g_{\mu+1}$ 分 7 种情况（前 4 种情况为 $g_{\mu+1} g_\mu = g_\mu g_{\mu+1}$ 的情况）来进行证明（下面的 δ 均表 ± 1）。

(1) $g_{\mu+1} = x_{1j}^\delta$，$\delta = \pm 1$，$j \geqslant 3$，不失一般地可设 $j = 3 = n$，此时

$$(a, b, c) g_{\mu+1} = (a, b, \delta a + c)$$

由此可定出 δ 的符号（$\pm$）使 $|c| > |\delta a + c|$，即 $\sigma_\mu > \sigma_{\mu+1}$。由于

$$g_\mu g_{\mu+1} = x_{12} x_{13}^\delta = x_{13}^\delta x_{12}，将$$

$$(a, b-a, c) \xrightarrow[g_\mu]{} (a, b, c) \xrightarrow[g_{\mu+1}]{} (a, b, \delta a + c)$$

代之以

$$(a, b-a, c) \xrightarrow[x_{13}^\delta]{} (a, b-a, \delta a + c) \xrightarrow[x_{12}]{} (a, b, \delta a + c),$$

则 $\sigma_\mu = \|(a,b,c)\|$ 变成 $\sigma_\mu' = \|(a, b-a, \delta a + c)\|$。显然 $\sigma_{\mu-1} > \sigma_\mu'$，而其余相邻的 σ_α 间的大小关系（因都用到 $g_\mu g_{\mu+1}$，或者都不用到 $g_\mu g_{\mu+1}$）都不变，于是使 $(\lambda, \mu) \downarrow$。

(2) $g_{\mu+1} = x_{ij}^\delta$，$i, j > 2$，仿(1)进行使 $(\lambda, \mu) \downarrow$。

(3) $g_{\mu+1} = g_\mu^\delta = x_{12}^\delta$。

$\delta = -1$ 时 $g_\mu g_{\mu+1} = 1$，消去后当然使 $(\lambda, \mu) \downarrow$。

$\delta = 1$ 不可能（因为 $(a,b,c) \xrightarrow[g_{\mu+1}]{} (a, b+a, c)$，从而

$$|b-a| \leqslant |b| > |b+a|,$$

这不可能）。

(4) $g_{\mu+1} = x_{32}^\delta$（或更一般地为 x_{i2}^δ，$i \geqslant 3$），此时

$$x_{12} x_{32}^\delta = x_{32}^\delta x_{12} = x_{13}^\delta x_{32}^\delta x_{13}^{-\delta} = x_{31}^\delta x_{12} x_{31}^{-\delta},$$

$$(a, b-a, c) \xrightarrow[x_{12}]{} (a, b, c) \xrightarrow[x_{32}^\delta]{} (a, b+\delta c, c),$$

因此 $|b| > |b + \delta c|$。用下面的（Ⅰ）、（Ⅱ）、（Ⅲ）之一代替：

（Ⅰ）$(a, b-a, c) \xrightarrow[x_{32}^\delta]{} (a, b-a+\delta c, c) \xrightarrow[x_{12}]{} (a, b+\delta c, c)$，

（Ⅱ）$(a, b-a, c) \xrightarrow[x_{13}^\delta]{} (a, b-a, c+\delta a) \xrightarrow[x_{32}^\delta]{} (a, b+\delta c, c+\delta a) \xrightarrow[x_{13}^{-\delta}]{} (a, b+\delta c, c)$，

(Ⅲ) $(a,b-a,c)\xrightarrow[x_{31}^{\delta}]{}(a+\delta c,b-a,c)\xrightarrow[x_{12}]{}(a+\delta c,b+\delta c,c)\xrightarrow[x_{31}^{-\delta}]{}(a,b+\delta c,c)$。

用(Ⅰ)代替时,在$|b-a|>|b-a+\delta c|$条件下$(\lambda,\mu)\downarrow$,

用(Ⅱ)代替时,在$|c|>|c+\delta a|$条件下$(\lambda,\mu)\downarrow$,

用(Ⅲ)代替时,在$|a|>|a+\delta c|$条件下$(\lambda,\mu)\downarrow$。

下证这三个条件至少有一个成立即可。事实上,由$|b|>|b+\delta c|$可知$b(\delta c)<0$。

当$a\neq 0$时,由(*)知$ab>0$,因此$a(\delta c)<0$。故$|c|>|c+\delta a|$或$|a|>|a+\delta c|$。

当$a=0$时,$|b-a|>|b-a+\delta c|$(因$b(\delta c)<0$),于是$|b-a|>|b-a+\delta c|$。由此知,对情况(4),总可使$(\lambda,\mu)\downarrow$。

(5) $g_{\mu+1}=x_{21}^{\delta}$,此时只用到第一、第二坐标。

$$(a,b-a)\xrightarrow[x_{12}]{}(a,b)\xrightarrow[x_{21}^{\delta}]{}(a+\delta b,b),\ |a|>|a+\delta b|。$$

$\delta=1$时,$ab<0$,与(*)中$ab>0$矛盾,因此必有$\delta=-1$。

用$x_{21}w_{21}(-1)$代替$x_{12}x_{21}^{-1}$,将$w_{21}(-1)$归入$g_{\mu+2}g_{\mu+3}\cdots g_m$部分。由

$$(a,b-a)\xrightarrow[x_{21}]{}(b,b-a)$$

并注意$|b|+|b-a|<|a|+|b|$知,$(\lambda,\mu)\downarrow$。

(6) $g_{\mu+1}=x_{23}^{\delta}$(或更一般地为$x_{2j}^{\delta},j\geqslant 3$),仿情况(4)之证。

(7) $g_{\mu+1}=x_{31}^{\delta}$(或更一般地为$x_{i1}^{\delta},i\geqslant 3$),此时

$$x_{12}x_{31}^{\delta}=x_{31}^{\delta}x_{12}x_{32}^{-\delta}=x_{31}^{\delta}x_{13}^{-\delta}x_{32}^{-\delta}x_{13}^{\delta},$$

$$(a,b-a,c)\xrightarrow[x_{12}]{}(a,b,c)\xrightarrow[x_{31}^{\delta}]{}(a+\delta c,b,c),$$

$$(a,b-a,c)\xrightarrow[x_{31}]{}(a+\delta c,b-a,c)\xrightarrow[x_{12}]{}(a+\delta c,b+\delta c,c)\xrightarrow[x_{32}^{-\delta}]{}(a+\delta c,b,c),$$

$$(a,b-a,c)\xrightarrow[x_{31}^{\delta}]{}(a+\delta c,b-a,c)\xrightarrow[x_{13}^{-\delta}]{}(a+\delta c,b-a,-\delta a)\xrightarrow[x_{32}^{-\delta}]{}(a+\delta c,b,-\delta a)\xrightarrow[x_{13}^{\delta}]{}(a+\delta c,b,c)。$$

由此知,$|b+\delta c|\leqslant|b|$或$|c|\geqslant|a|$时$(\lambda,\mu)\downarrow$。但由$\sigma_{\mu}>\sigma_{\mu+1}$知$|a|>|a+\delta c|$,因此$a(\delta c)<0$且$|c|<2|a|$。于是$b(\delta c)<0$(因由(*)知$ab>0$)。由此知,或$|c|\leqslant 2|b|$,因此$|b+\delta c|\leqslant|b|$;或$|c|>2|b|$,因此由(*)知,此时$|c|\geqslant|a|$,于是总可使$(\lambda,\mu)\downarrow$。综上即得欲证。 □

引理 31.4 设$n\geqslant 2$,$\phi_n=\phi|_{\mathrm{St}_n(\mathbb{Z})}:\mathrm{St}_n(\mathbb{Z})\to\mathrm{E}_n(\mathbb{Z})$,则

$$\mathrm{Ker}\phi_n \subseteq \mathrm{W}_n$$

证 由上两引理可知 $\forall X = g_1 g_2 \cdots g_m w \in \mathrm{St}_n(\mathbb{Z}) \cap \mathrm{Ker}\phi_n$，其中 $w \in \mathrm{W}_n, g_k \in \{x_{ij}^{\pm 1}\}$

$$1 \leqslant \|\beta g_1\| \leqslant \|\beta g_1 g_2\| \leqslant \cdots \leqslant \|\beta g_1 g_2 \cdots g_m w\| = 1$$

于是有

$$\|\beta g_1\| = \|\beta g_1 g_2\| = \cdots = \|\beta g_1 g_2 \cdots g_m\| = 1,$$

$$\forall \pm\beta \text{ 为 } \mathbb{Z}^n \text{ 的标准正交基。}$$

由于 β 可取任意的 $\mathbb{Z}^n$ 的标准正交基中向量。因此 $g_1 = 1, g_1 g_2 = 1 \cdot g_2 = 1, \cdots, g_1 g_2 \cdots g_m = 1$。于是 $X = 1 \cdot w = w \in \mathrm{W}_n$，即 $\mathrm{Ker}\phi_n \subseteq \mathrm{W}_n$。□

现在可证

命题 31.6 设 $n \geqslant 3$，则 $\mathrm{St}_n(\mathbb{Z})$ 为 $\mathrm{E}_n(\mathbb{Z})$ 的中心扩张且有正合列

$$1 \to \mathrm{C}_n \to \mathrm{St}_n(\mathbb{Z}) \xrightarrow[\phi_n]{} \mathrm{E}_n(\mathbb{Z}) \to 1,$$

且 $\mathrm{C}_n = \langle\{-1,-1\}\rangle \simeq \mathbb{Z}_2$，其中 $\{-1,-1\} = (x_{12} x_{21}^{-1} x_{12})^4$。

证 由上引理已知 $\mathrm{Ker}\phi_n \subseteq W_n$. 又由 §26 知

$$\mathrm{C}_n = \mathrm{Ker}(\phi|_{w_n}) \subseteq C(\mathrm{St}_n(\mathbb{Z}))$$

但 $\mathbb{Z}^{\cdot} = \{\pm 1\}$，$\{1, \mathbb{Z}^{\cdot}\} = 1$，于是 $\mathrm{C}_n = \langle\{-1,-1\}\rangle \simeq \mathbb{Z}_2$（由命题 31.4 已知在 $\mathrm{K}_2\mathbb{Z}$ 中 $\mathrm{ord}\{-1,-1\} = 2$）。□

定理 31.2 $\mathrm{K}_2\mathbb{Z} = \langle\{-1,-1\}\rangle \simeq \mathbb{Z}_2$。

证 由引理 31.4 可得

$$\mathrm{C} = \mathrm{W} \cap \mathrm{Ker}\phi = \mathrm{Ker}\phi = \mathrm{K}_2\mathbb{Z}$$

再由上命题取（正向）极限即得证。□

由此定理与定理 10.4 立得

推论 31.3 $\mathrm{K}_2\mathbb{Z}^{n \times n} \simeq \mathbb{Z}_2$。

命题 31.6 事实上可改写为

命题 31.6′ 设 $n \geqslant 3$，记 $e_{ij} = e_{ij}^1$，则

$$\mathrm{SL}_n(\mathbb{Z}) = \mathrm{E}_n(\mathbb{Z}) = \left\langle \left\{ e_{ij} \;\middle|\; \begin{array}{l} [e_{ij}, e_{kl}] = \begin{cases} 1, & j \neq k, i \neq l \\ e_{ik}, & j = k, i \neq l \end{cases} \\ (e_{12} e_{21}^{-1} e_{12})^4 = 1 \end{array} \right\} \right\rangle。$$

对 $n = 2$，注意在 $\mathrm{St}_2(\mathbb{Z})$ 中，$w_{12} w_{21} = 1$，因此 W_2 为循环群。而由 $\mathrm{ord}\,\phi(w_{12}) = 4$ 又知 $\mathrm{Ker}\phi = \langle (w_{12})^4 \rangle$，可证有类似于命题 31.6 的下述结果。

命题 31.7 $\mathrm{St}_2(\mathbb{Z})$ 为 $\mathrm{E}_2(\mathbb{Z})$ 的中心扩张，且有正合列

$$1 \to \mathrm{C}_2 \to \mathrm{St}_2(\mathbb{Z}) \xrightarrow[\phi_2]{} \mathrm{E}_2(\mathbb{Z}) \to 1,$$

其中 $\mathrm{C}_2 = \langle (x_{12} x_{21}^{-1} x_{12})^4 \rangle \simeq \mathbb{Z}$，因此

$$SL_2(\mathbb{Z}) = E_2(\mathbb{Z}) = \langle\left\{e_{12}, e_{21}\ \middle|\ \begin{array}{l} e_{12}e_{21}^{-1}e_{12} = e_{21}^{-1}e_{12}e_{21}^{-1} \\ (e_{12}e_{21}^{-1}e_{12})^4 = 1 \end{array}\right\}\rangle。$$

上述的命题 31.3 在相对 K 理论中也有重要的应用。比如,我们可用它推出著名的 Mennicke-Bass-Lazard-Serre 定理。为此先介绍一些概念与记号。

设 $R \in \text{Ring}, A \lhd R, \pi: \twoheadrightarrow S = R/A$ 为标准环同态,则得一环

$$D = \{(r_1, r_2) \mid r_j \in R \text{ 且 } \pi(r_1) = \pi(r_2)\}$$
$$= \{(r_1, r_2) \in R \times R \mid r_1 \equiv r_2 \pmod{A}\}$$

称 D 为 R 在 A 上的**双环**(double ring)。

显然有环的满同态组成的 Descartes 方图

$$\begin{array}{ccc} D & \xrightarrow{p_2} & R \\ {\scriptstyle p_1}\downarrow & & \downarrow{\scriptstyle \pi} \\ R & \xrightarrow[\pi]{} & S = R/A \end{array}$$

其中 $p_j((r_1, r_2)) = r_j, j = 1, 2$。

参照§9,记

$$K_i(R, A) = \text{Ker}(K_i p_2),\ i = 0, 1$$

称为 R 关于 A 的**相对 K_i 群**(relative K_i-group)。记

$$GL(R, A) = \text{Ker}(GL(\pi)) = \{X \in GL(R) \mid X \equiv I \pmod{A}\},$$
$$E(R, A) = \langle\{e_{ij}^x \mid x \in A, i \neq j\}\rangle。$$

可证

$$K_1(R, A) \simeq GL(R, A)/E(R, A)$$
$$\simeq GL(R, A)/[GL(R), GL(R, A)]$$

注意上图中 π 为满同态,由§18 中 K_1, K_2 群的正合列,可得下行正合的交换图:

$$\begin{array}{ccccccccccc} K_1(R,A) & \xrightarrow{K_1 p_1} & K_1 R & \xrightarrow{K_1 \pi} & K_1 S & \xrightarrow{\delta} & K_0(R,A) & \xrightarrow{K_0 p_1} & K_0 R & \xrightarrow{K_0 \pi} & K_0 S \\ \downarrow & & \downarrow{\scriptstyle i_1} & & \| & & \downarrow & & \downarrow{\scriptstyle i_0} & & \| \\ K_1 D & \xrightarrow[f_1]{} & K_1 R \oplus K_1 R & \xrightarrow[g_1]{} & K_1 S & \xrightarrow[\delta]{} & K_0 D & \xrightarrow[f_0]{} & K_0 R \oplus K_0 R & \xrightarrow[g_0]{} & K_0 S \end{array}$$

其中 i_0, i_1 表示到第一直和项的标准单射:$x \mapsto (x, 0)$。用图追踪法(见[佟文廷,1998])知,上行也是正合的。注意上面的 Descartes 方图中 π 为满同态,由上图下行又可向左延长为 K_2, K_1, K_0 群的九项正合列(见§18 注①)。由此即得

命题 31.8 设 $R\in\mathbb{R}\text{ing}$，$A\lhd R$，且 $\pi:R\twoheadrightarrow S=R/A$ 为标准环同态，则有正合列(其中 σ,δ 为连结同态)

$$\mathrm{K}_2R\xrightarrow[\mathrm{K}_2\pi]{}\mathrm{K}_2S\xrightarrow[\sigma]{}\mathrm{K}_1(R,A)\xrightarrow[\mathrm{K}_1p_1]{}\mathrm{K}_1R\xrightarrow[\mathrm{K}_1\pi]{}$$
$$\mathrm{K}_1S\xrightarrow[\delta]{}\mathrm{K}_0(R,A)\xrightarrow[\mathrm{K}_0p_1]{}\mathrm{K}_0R\xrightarrow[\mathrm{K}_0\pi]{}\mathrm{K}_0S$$

对交换环 R，又可记

$\mathrm{SL}(R,A)=\{X\in\mathrm{GL}(R,A)\mid\det X=1\}$，

$\mathrm{SK}_1(R,A)=\mathrm{SL}(R,A)/\mathrm{E}(R,A)$(相对特殊 K_1 群)，

$\mathrm{U}(A)=(R/A)^{\cdot}=\{r\in R^{\cdot}\mid r\equiv 1\pmod{A}\}$(显然 $\mathrm{U}(R)=R^{\cdot}$)。

由定理 5.3′，我们已知对 $R\in\mathbb{C}\text{Ring}$，

$$\mathrm{K}_1R\simeq R^{\cdot}\oplus\mathrm{SK}_1R,\quad \text{其中 }\mathrm{SK}_1R=\mathrm{SL}(R)/\mathrm{E}(R)。$$

类似地，可以证明

$$\mathrm{K}_1(R,A)\simeq\mathrm{U}(A)\oplus\mathrm{SK}_1(R,A)$$

注意 $\mathrm{K}_1(R,A)\xrightarrow[\mathrm{K}_1p_1]{}\mathrm{K}_1R\xrightarrow[\mathrm{K}_1\pi]{}\mathrm{K}_1S$ 相当于 $\mathrm{U}(A)\rightarrowtail R^{\cdot}\to S^{\cdot}$ 与 $\mathrm{SK}_1(R,A)\to\mathrm{SK}_1R\to\mathrm{SK}_1S$，且由 $\mathrm{U}(A)\rightarrowtail R^{\cdot}$ 知，$\mathrm{Ker}(\mathrm{K}_1P_1)\subseteq\mathrm{SK}_1(R,A)$。于是可得

引理 31.5 设 $R\in\mathbb{C}\text{Ring}$，$A\lhd R$，且 $\pi:R\twoheadrightarrow S=R/A$ 为标准环同态，则有正合列

$$\mathrm{K}_2R\xrightarrow[\mathrm{K}_2\pi]{}\mathrm{K}_2S\xrightarrow[\sigma']{}\mathrm{SK}_1(R,A)\to\mathrm{SK}_1R\xrightarrow[\mathrm{SK}_1\pi]{}\mathrm{SK}_1S$$

由此可证

命题 31.9 (Mennicke-Bass-Lazard-Serre 定理)

$$\mathrm{SK}_1(\mathbb{Z},n\mathbb{Z})=1,\ \forall n>1$$

证 令 $R=\mathbb{Z}$，$A=n\mathbb{Z}$，$S=\mathbb{Z}_n$，由命题 31.3 知 $\mathrm{K}_2\pi:\mathrm{K}_2\mathbb{Z}\to\mathrm{K}_2\mathbb{Z}_n$ 为满同态。因此，由引理 31.5 得行正合交换图

$$\begin{array}{ccccccccc}
\mathrm{K}_2R & \xrightarrow{\mathrm{K}_2\pi} & \mathrm{K}_2S & \xrightarrow{\sigma'} & 1 & \longrightarrow & \mathrm{SK}_1R & \xrightarrow{\mathrm{SK}_1\pi} & \mathrm{SK}_1S\\
\| & & \| & & \downarrow & & \| & & \|\\
\mathrm{K}_2R & \xrightarrow[\mathrm{K}_2\pi]{} & \mathrm{K}_2S & \xrightarrow[\sigma']{} & \mathrm{SK}_1(R,A) & \to & \mathrm{SK}_1R & \xrightarrow[\mathrm{SK}_1\pi]{} & \mathrm{SK}_1S
\end{array}$$

由 5—引理(见[佟文廷，1998])即知 $\mathrm{SK}_1(R,A)=1$。 □

用引理 31.5 还可证

命题 31.10 设 O_F 为代数数域 F 的代数整元环，$P\in\mathrm{Spec}\ \mathrm{O}_F$，则

$$\mathrm{SK}_1(\mathrm{O}_F,P)=1$$

证 用引理 31.5 中的正合列(取 $S=\mathrm{O}_F/P$)，注意 S 为有限域(由引理

7.4),因此 $K_2S=1$(定理 26.2),当然更有 $SK_1S=1$,则知

$$SK_1(O_F,p)\simeq SK_1(O_F)$$

但由§5 注 1 中 Milnor-Serre 的结果:$SK_1(O_F)=1$,故

$$SK_1(O_F,P)=1$$

参 考 文 献

王芳贵. 本原环的 Grothendieck 群. 数学学报,34(5)(1991): 645—652

冯克勤. 代数数论入门. 上海:上海科技出版社,1988

陈胜,游宏. 虚二次域整环的 K_2 群的计算. 中国科学(A 辑),31(3)(2001): 222—229

陈焕良. Grothendieck 群及其应用. 南京大学博士论文,1994

陈焕良,佟文廷. 正则环的幂问题. 数学学报,41(6)(1997): 815—822

宋光天. 半群的代数 K 理论(I)——半群的 Grothendieck 群. 数学学报,33(3)(1990): 309—322

佟文廷. 关于 IBN 环的一些结果. 南京大学学报数学半年刊,1(2)(1984): 217—223

佟文廷. Grothendieck 群及其应用. 南京大学学报数学半年刊,3(1)(1986): 1—11

佟文廷. 关于有限生成投射模为自由模的环. 数学研究与评论,9(3)(1989): 319—323

佟文廷. 同调代数引论. 北京:高等教育出版社,1998

周伯勋. 代数 K 理论的起源与发展概况. 南京大学学报数学半年刊,1(1987): 91—98

周伯勋. 同调代数. 北京:科学出版社,1988,1998

武同锁. 稳定列条件与 K_0 函子. 南京大学博士论文,1994

柯召,孙琦. 谈谈不定方程. 上海:上海教育出版社,1980

秦厚荣. K_2 群和代数数论. 南京大学博士论文,1992

秦厚荣. 关于域的 K_2 群的有限阶元素. 科学通报,38(1)(1993): 2227—

2229

秦厚荣.实二次域的整元环上的 K_2 群.中国科学(A辑),23(1993):1254—1263

郭学军.相对 K_1,K_2 和代数整数环的 K_2.中国科技大学博士论文,2000

日本数学会编集.岩波数学辞典(日文).第3版.岩波书店,1985

唐向东.交换环的 Picard 群上的相容预序格.南京大学学报数学半年刊,17(2)(2000):250—253

潘承洞,潘承彪.初等代数数论.济南:山东大学出版社,1991

Ara, P.. Extensions of exchange rings. J. of Algebra, 197(1997): 409—423

Ara, P., Goodearl, K. R., O'meara, K. C. and Pardo, E.. Seperative cancellation for projective modules over exchange rings. Israel J. Math., 105(1998): 105—137

Auslander, M.. Relations for Grothendieck groups of artin algebras. Proc. Amer. Math. Soc., 293(1984): 336—340

Bass, H.. K-theory and stable algebra. Publ. IHES., 22(1964): 5—60

Bass, H.. Algebraic *K*-Theory. W. A. Benjamin, New York and Amsterdam, 1968

Berrick, A. J.. An Approach to Algebraic *K*-Theory. Res. Notes in Math. 56, Pitman, Boston, Mass., 1982

Berrick, A. J., Keating, M. E.. An Introduction to Rings and Modules with *K*-Theory in view. Cambridge Univ. Press, 2000

Blackadar, B.. *K*-Theory for Operator Algebra. Math. Sci. Res. Inst. Pub., 5, Springer-Verlag, New York Inc., 1986

Browkin, J.. Elements of small order in K_2F, in Algebraic *K*-Theory. Lecture Notes in Math., 966: 1—6, Springer-Verlag, Berlin-Heidelberg-new York, 1982

Browkin, J.. The functor K_2 of the ring of integers of a number fields, in Universal Algebra and Applications. Banach Center Publ. 9: 187—195, PWN, Warsaw, 1982

Butler, M. C. R.. Grothendieck groups and almost split sequences, Proc. Oberwolfach. Lecture Notes in Math. 882, 357—368, Springer-Verlag, Berlin-Heidelberg-New York, 1980

Camps, R., Dicks, W.. On semilocal rings. Israel J. Math., 81(1993): 203—211

Chen, H. Y., Tong, W. T.. Category $X\mathscr{L}(R)$ and $X\mathscr{L}$-groups. Sci. in China, Ser. A, 38(2)(1995): 159—170

Chen, H. Y., Tong, W. T.. Finitely generated projective modules over Abelian group rings. Chin. J. of Contemp. Math., 16(3)(1995): 215—225

Chen, H. Y., Tong, W. T.. On projective free properties of rings. Sci. in China, Ser. A, 39(2)(1996): 177—186

Chen, H. Y.. Rings with stable range conditions. Comm. in Algebra, 26 (11)(1998): 3653—3668

Chen, H. Y.. On stable range conditions. Comm. in Algebra, 28(8) (2000): 3913—3924

Chen, H. Y., Li, F. A.. Rings with many unit-regular elements. Chin. J. of Contemp. Math., 21(1)(2000): 33—38

Chen, H. Y.. Units, idempotents, and stable range conditions. Comm. in Algebra, 29(2)(2001): 703—717

Claborn, L.. Every abelian group is a class group. Pacific J. Math., 18 (1966): 219—222

Cohn, P. M.. The complement of a finitely generated direct summand of an Abelian group. Proc. Amer. Math. Soc., 7(1956): 520—521

Cohn, P. M.. Algebra, vol. 2, John Wiley & Sons, Chichester, New York, 1979

Feng, K. Q.. On the Birch-Tate conjecture for cyclic mumber field. J. Pure and Appl. Algebra, 48(1987): 223—228

Feng, L. G.. Finitely generated modules and power stably free dimension. Comm. in Algebra, 29(12)(2001): 5335—5343

Gillman, L., Jerison, M.. Rings of continuous Functions. GTM, 43, Springer-Verlag, New York, 1976

Goodearl, K. R.. Cancellation of low-rank vector bundles. Pacific J. Math., 113(1984): 289—302

Goodearl, K. R.. Von Neumann Regular Rings, 2nd Ed.. Krieger Publ. Co., Malabar, Florida, 1991

Hasse, H.. Number Theory. Springer-Verlag, Berlin, 1980

Hirzebruch, F.. Division algebras and topology, in Numbers. GTM, 123:281—328, Springer-Verlag, New York, 1991

Hungerford, T. W.. Algebra. GTM, 73, Springer-Verlag, New York, 1980

Inassaridze, H., Ed.. *K*-Theory and Homological Algebra. Lecture Notes in Math., 1437, Springer-Verlag, Berlin, 1990

Ireland, K., Rosen, M.. A Classical Introduction to Modern Number Theory. GMT, 84, Springer-Verlag, New York, 1982

Karpilovsky, G.. Commutative Group Algebras. Marcel Dekker, Inc., New York and Basel, 1983

Kolster, M.. The structure of the 2-Sylow subgroup of $K_2(O)$. I, Comment. Math. Helv., 61(1986): 376—388

Lam, T. Y.. Serre's Conjecture, Lecture Notes in Math.. 635, Springer-Verlag, Berlin, Heidelberg, New York, 1978

Lam, T. Y.. Lecture on Rings and Modules, 2nd ed.. GTM, 189, Springer-Verlag, New York, 1999

Lam, T. Y., Magid, A. R. (Ed.). Algebra, K-Theory. Groups and Education, Contemp. Math., 243, AMS, Providence, 1999

Li, F. A., Liu, M. L.. A generalized sandwich theorem, K-Theory, 1(2) (1987): 171—183

Li, F. A.. Isomorphisms of Steinberg groups over commutative rings. Acta Math. Sinica (New Ser.), 5(2)(1989): 146—158

Li, F. A.. Decompostion of Steinberg groups. Chinese Science Bulletin, 37(15)(1992): 1244—1248

Liu, M. L.. The group $G_1(R\Pi)$ for Π a finite Abelian group. J. of Pure and Appl. Algebra, 24(1982): 287—291

Liu, Z. K.. Hermite and PS-rings of Hurwitz series. Comm. in Algebra, 28(1)(2000): 299—305

Long, R. L.. Algebraic Number Theory. Marcel Dekker, Inc., New York and Basel, 1977

Marcos, E. N., Merklen, H. A., Platzeck, M. I.. The Grothendieck group of the category of modules of finite projective dimension over certain weakly triangular algebras. Comm. in Algebra, 28(3) (2000): 1387—1404

Matsumura, H.. Commutative Ring Theory. Translated by Reid, M., Cambridge Univ. Press, 1989

Mazur, B., Wiles, A.. Class fields of abelian extensions of Q. Invent. Math., 76(1984): 179—330

McConnell, J. C., Robson, J. C.. Noncommutative Noetherian Rings. John Wiley & Sons. Chichester, New York, 1988

McDonald, B. R.. Linear Algebra over Commutative Rings. Marcel Dekker, Inc., New York and Basel, 1984

Menal, P., Moncasi, J.. K_1 of von Neumann regular rings. J. Pure and Appl. Algebra, 33(1984): 295—312

Menal, P.. Cancellation modules over regular rings, in *Proc. of Canada Ring Theory Conf.*. Lecture Notes in Math., 1328: 187—209, 1988

Milnor, J.. Introduction to Algebraic K-Theory. Annals of Math. Studies, 72, Princeton, 1971

Oliver, R.. Whitehead Groups of Finite Groups. London Math. Soc. Lecture Notes Series, 132, Cambridge Univ. Press, Cambridge, 1988

Orzech, G., Orzech, M.. Plane Algebraic Curves. PAM, 61, Marcel Dekker, Inc., New York and Basel, 1981

Quillen, D.. Projective modules over polynomial rings. Invent. Math., 36(1976): 167—171

Qin, H. R.. Comptation of $K_2\mathbf{Z}[\sqrt{-6}]$. J. Pure and Appl. Algebra, 96 (1994), 133—146

Qin, H. R.. 2-Sylow subgroups of K_2O_F for real quadratic fields F. Sci. in China (Ser. A), 37(11)(1994): 1302—1313

Qin, H. R.. The 2-sylow subgroups of the tame kernel of imaginary quadratic fields. Acta Arith., LXIX(2)(1995): 153—169

Qin, H. R.. Computation of $K_2\mathbf{Z}\frac{1+\sqrt{-35}}{2}$. Chin. Ann. of Math., 17 (B)(1)(1996): 63—72

Ribenboim, P.. The Book of Prime Number Records, 2nd Ed.. Springer-Verlag, 1989

Rosenberg, J.. Algebraic K-Theory and its Applications. GTM, 147, Springer, 1994

Rotman, J. J.. An Introduction to Homological Algebra. Acad. Press, New York, 1979

Rudin, W.. Unique right inverses are two-sided. Amer. Math. Monthly, 8—9(1985): 489—490

Serre, J. P.. Faisceaux algebriques cohérents. Ann. Math., 61(1955): 191—278

Silvester, J. R.. Introduction to Algebraic K-Theory. Chapman and Hall, London and New York, 1981

Steger, A.. Diagonability of idempotent matrices. Pacific J. Math., 19 (3)(1966): 535—541

Suslin, A. A.. Projective modules over a polynomial ring are free. Dokl. Akad. Nauk. SSSR, 229(1976)(=Soviet Math. Dokl., 17(1976)): 1160—1164

Suslin, A. A.. Torsion in K_2 of fields. K-Theory, 1(1987): 5—29

Suzuki, M.. Group Theory. I, GMW. 247, Springer-Verlag, Berlin, New York, 1982

Swan, R. G.. Vector bundles and projective modules. Trans. Amer. Math. Soc., 105(1962): 264—277

Swan, R. G.. Algebraic K-Theory. Lecture Notes in Math., 76, Springer, 1968

Swan, R. G.. Vector bundles, projective modules and the K-theory of spheres, in *Algebraic Topology and Algebraic K-Theory*. Ed. by W. Browder, Ann. of Math. Studies, 113, Princeton Univ. Press, 432—522

Tate, J.. Relations between K_2 and Galois cohomology. Invent. Math., 36(1976): 257—274

Tong, W. T.. On Euler characteristic of modules. Chin. Ann. Math., 10B(1)(1989): 58—63

Tong, W. T.. IBN rings and orderings on Grothendieck groups. Acta Math. Sinica(New Ser.), 10(3)(1993): 225—230

Tong, W. T.. Connected PT rings. Algebra Colloq., 1(3)(1994): 267—270

Urbanowitz, J.. On elements of given orders in K_2F. J. Pure and Appl. Algebra, 50(1988): 295—307

Vaserstein, L. N.. Vector bundles and projective modules. Trans. Amer. Math. Soc., 294(1986): 749—755

Walker, E. A.. Cancellation in direct sum of groups. Proc. Amer. Math.

Soc., 7(1956): 898—902

Washington, L. N.. Introduction to Cyclotomic Fields. GTM, 83, Springer-Verlag, New York, 1982

Wiles, A.. The Iwasawa conjecture for totally real number fields. Ann. of Math., 131(1990): 493—450

Wu, T.S.. U1—sr conditions. Chin. Ann. Math., 16A(6)(1995): 760—768

Wu, T.S., Tong, W.T.. Stable range condition and cancellation of modules, in Pitman Res. Notes Math. Ser., 346(1996), 98—104, Pitman, London

Wu, T.S., Tong, W.T.. Finitely generated projective modules over exchange rings. Manus. Math., 86(2)(1995): 149—157

Wu, T. S., Xu, Y. H.. On the range condition of exchange rings. Comm. in Algebra, 25(7)(1997): 2355—2363

Xu, K.J., Qin, H.R.. A conjecture on a class of elements of finite order in K_2F_p. Sci. in China, Ser. A, 31(1)(2001): 11—17

Xue, W.M.. Rings with Morita Duality. Lecture Notes in Math., 1523, Springer-Verlag, 1992

You, H.. $K_2(R,I)$ of unit 1-stable ring. Chin. Sci. Bull., 35(19)(1990): 1590—1595

You, H.. Some remarks on decompositions of Steinberg groups. Chin. Sci. Bull., 37(18)1992: 1645—1649

Yue, Q.. The structure of certain K_2O_F. J. Math. Res. Exp., 21(1)(2001): 1—6

Zhou, B.X., Tong, W.T.. Some progress in algebraic K-Theory in China, in *Rings, Groups, and Algebras*. Lecture Notes in Pure and Appl. Math., 181, Marcel Dekker, Inc., New York, Basel, Hong Kong, 1996

Zhu, X.S.. Tong, W.T., Categories of power stable free modules and their K_0 groups. Sci. in China, Ser. A, (1997), 40(12): 1239—1246

Zhu, X. S.. Power stably free resolutions and Grothendieck groups. Comm. in Algebra, 29(7)(2001): 2899—2921

Боревич, З. И., Шафаревич, И. Р.. Теория чисел, Издательство. *НАУКА*, Москва, 1964

名 词 索 引

（汉语拼音序）

【D】

【E】

【F】

【G】

【H】

【L】

【M】

【N】

【P】

【Q】

【R】

【S】

【T】

【U】

【W】

【X】

【Y】

【Z】

记　号　表

（按**“范畴”**、**“函子”**、**“模”**、**“群”**、**“环”**、**“其他”**分类排列）

【范畴】

AG （Abel 群范畴）

Bun(B) （拓扑空间 B 上的丛范畴）

CRing （有单位元的交换环范畴）

f. g. $_R\mathfrak{M}$ （有限生成左 R-模范畴）

f. g. $\mathrm{Free}_R\mathfrak{M}$ （有限生成自由左 R-模范畴）

f. g. $P_R\mathfrak{M}$ （有限生成投射左 R-模范畴）

f. p. $_R\mathfrak{M}$ （有限表示左 R-模范畴）

f. p. r. $_R\mathfrak{M}$ （有有限投射分解的左 R-模范畴）

f. t. Vec(X) （拓扑空间 X 上的有限型向量丛范畴）

G （群范畴）

$P_R\mathfrak{M}$ （投射左 R-模范畴）

Ring （有单位元环的范畴）

Rng （不要求有单位元的环范畴）

$SF_R\mathfrak{M}$ （稳定自由左 R-模范畴）

Vec(B) （拓扑空间 B 上的向量丛范畴）

$\Omega\mathcal{P}$ （范畴 $\mathcal{P}$ 的回路范畴）

【函子】

ab, *ab* （群的 Abel 化函子）

E （初等(矩阵)群函子）

E_n （n 阶初等(矩阵)群函子）

Ext_R^n （Hom_R 的第 n 个右导出函子）

GL （一般线性群函子）

GL_n （n 阶一般线性群函子）

K_i （K_i 群函子，i=0,1,2,…）
H_0 （Spec R 的二值连续函数群函子）
H_n （第 n 个同调函子）
H^n （第 n 个上同调函子）
Hom_R （关于 R-模同态的 Hom 函子）
$\varinjlim$ （正向极限函子）
$\varprojlim$ （反向极限函子）
Pic （Pic 群函子）
S^{-1} （局部化函子）
SK_1 （特殊 K_1 群函子）
St （Steinberg 群函子）
St_n （n 阶 Steinberg 群函子）
Tor_n^R （张量积函子$\otimes_R$的第 n 个左导出函子）
$\otimes_R$ （张量积函子）
$\widetilde{K}_0$ （约化(K_0 群)函子）

【模】

FFR （有有限长有限自由分解的模）
$M^* = Hom_R(M,R)$ （R-模 M 的对偶模）
M_p （模 M 在素理想 P 的局部化）
$\wedge^p M$ （模 M 的 p 次外乘幂）
$\otimes^p M$ （模 M 的 p 次张量幂）
$\oplus^p M$ （p 个模 M 的直和）
$\langle P\rangle$ （有限生成投射模 P 的同构类）
$[P]$ （有限生成投射模 P 的稳定同构类）
rank$M$ （模 M 的常数秩，IBN 环上自由模 M 的秩）
$rank_p M$ （模 M 在素理想 P 的局部秩）
$S^{-1}M$ （模 M 关于环中乘法闭集 S 的局部化）
$\overset{s}{\simeq}$ （有限生成投射模间的稳定同构）
$\chi(M)$ （模 M 的 Euler 示性数）

【群】

$C=\bigcup C_n=<\{\{u,v\}\mid u,v\in R^*, uv=vu\}>$，$K_2(R)$的一个子群）
c. e. （群的中心扩张）
$C(G)$ （群 G 的中心）
$Cl(R)$ （整环 R 的理想类群）
$C_n=C_n(R)=Ker(\varphi|_{W_n})$（$K_2(R)$（$K_{2,n}(R)$）的一个子群）

$C(R)=C(R,R)=\langle\{\{u,v\}\mid u,v\in R^{\cdot}\}\rangle$ （交换环 R 的 K_2 群的一个子群）

$C(R,I)=K_2(R)\cap H(R,I)$ （R 为交换环时即$\langle\{\{u,v\}.\ u,v\in R^{\cdot},u,v\equiv 1\ (\mathrm{mod} I)\}\rangle$，$K_2(R)$关于理想 I 的子群）

$\mathfrak{C}(R)=\mathfrak{C}(R,R)=\langle\{\langle a,b\rangle\mid a,b\in R,1+ab\in R^{\cdot}\}\rangle$ （交换环 R 的 K_2 群的一个子群，R 又为局部环时即 $K_2(R)$）

$\mathfrak{C}(R,I)=K_2(R)\cap\mathfrak{H}(R,I)$ （R 为交换环时即$\langle\{\langle a,b\rangle\mid a\in I\lhd R,b\in R,1+ab\in R^{\cdot}\}\rangle$，$K_2(R)$关于理想 I 的子群）

$D_n(R)$ （环 R 上对角元为 $d\in R^{\cdot}$ 与 $1,\cdots,1$，的 n 阶对角阵群）

$D(R)$ （环 R 上对角元为 $d\in R^{\cdot}$ 与 $1,\cdots,1\cdots$的无穷阶对角阵群）

$D(V)$ （正规仿射数簇 V 的(Weil)除子群）

$E_n(R)$ （环 R 上的 n 阶初等(矩阵)群）

$E(R)$ （环 R 上的初等(矩阵)群）

$E(R,A)=\langle e_{ij}^{A}\mid i\neq j\rangle$ （环 R 相对于理想 A 的初等(矩阵)群）

$G^{ab}=G/[G,G]$ （群 G 的 Abel 化）

$GE_n(R)$ （环 R 上的 $E_n(R)$与 n 阶可逆(逆)对角阵生成的群）

$G_i(R)$ （环 R 的 G_i 群，即有限生成 R-模范畴的 K_i 群）

$GL_n(R)$ （环 R 上的 n 阶一般线性群）

$GL(R,A)=\{X\in GL(R)\mid X\equiv I\ (\mathrm{mod} A)\}$ （环 R 相对于理想 A 的一般线性群）

$G(S)$ （Abel 半群 S 的群完备化）

$H=\bigcup_{n=1}^{\infty}H_n$ （Steinberg 群 $St(R)$的一个子群）

$H_n=H_n(R)$ （Steinberg 群 $St(R)$中由 $H_{ij}(R^{\cdot})$生成的子群）

$H(R)=H(R,R)$ （环 R 的 Steinberg 群 $St(R)$的一个子群）

$H(R,I)=\langle\{h_{ij}(u)\mid i\neq j,u\in R^{\cdot}.u\equiv 1\ (\mathrm{mod}\ I)\}\rangle$ （环 R 的 Steinberg 群 $St(R)$关于理想 I 的一个子群）

$\mathfrak{H}(R)=\mathfrak{H}(R,R)$ （环 R 的 Steinberg 群 $St(R)$的一个子群）

$\mathfrak{H}(R,I)=\langle\{H_{ij}(a,b)\mid i\neq j,a\in I\lhd R,b\in R,1+ab\in R^{\cdot}\}\rangle$ （环 R 的 Steinberg 群 $St(R)$关于理想 I 的一个子群）

$H_n(G,M)=\mathrm{Tor}_n^{ZG}(Z,M)$ （群 G 的系数在ZG-模 M 中的第 n 个同调群）

$H^n(G,M)=\mathrm{Ext}_{ZG}^n(Z,M)$ （群 G 的系数在ZG-模 M 中的第 n 个上同调群）

$\mathrm{Idem}(R)$ （环 R 上对角线上由一有限阶幂等阵与无穷阶零矩阵组成的分块对角阵的等价类生成的半群）

$K_i(R)(K_iR)$ （环 R 的 K_i-群，$i=0,1,2,\cdots$）

$\widetilde{K}_0(R)$ （环 R 的约化 K_0-群）

$K_i(R,A)$ （环 R 的相对于理想 A 的 K_i 群，$i=0,1,2,\cdots$）

$K_{2,n}(R)$ （$St(R)$到 $E_n(R)$的标准同态的核）

$K^0(B)$ （拓扑空间 B 上向量丛范畴的 K_0 群）

$\mathrm{Pic}(R)$ （交换环 R 的 Picard 群）

Proj(R) （有限生成投射左 R-模同构类的半群）

P(V) （正规仿射代数簇 V 的主除子群）

$R^{\cdot}=\mathrm{U}(R)$ （环 R 的乘法群(可逆元群)）

$\mathrm{rK}_0(R)=\{[M]-[N]\in \mathrm{K}_0(R)\mid \mathrm{rank}_P M=\mathrm{rank}_P N,\forall P\in \mathrm{Spec}R\}$ （交换环 R 的 K_0 群的直和项，$\mathrm{H}_0(R)$的直和补）

$\mathrm{SK}_1(R)$ （交换环 R 的特殊 K_1 群）

$\mathrm{SK}_1(R,A)=\mathrm{SL}(R,A)/E(R,A)$ （交换环 R 的相对特殊 K_1 群，$A\lhd R$）

$\mathrm{SL}(R)$ （交换环 R 的特殊线性群）

$\mathrm{SL}_n(R)$ （交换环 R 的 n 阶特殊线性群）

$\mathrm{SL}(R,A)=\{X\in \mathrm{GL}(R,A)\mid \det X=1,A\lhd R\}$ （交换环 R 的相对特殊线性群）

$\mathrm{St}(I)=\langle x_{ij}(I)\mid i\neq j,I\lhd R\rangle$ （St(R)的一个子群）

$\mathrm{St}_n(R)$ （环 R 的 n 阶 Steinberg 群）

$\mathrm{St}(R)$ （环 R 的 Steinberg 群）

$\mathrm{St}(R,I)=\mathrm{Ker}(\mathrm{St}(R)\rightarrow \mathrm{St}(R/I))$

$T=T(R)=\langle\{x_{ij}(a)\mid i<j,a\in R\}\rangle$ （St(R)的上三角子群）

$T'=T'(R)=\langle x_{ij}(a)\mid i>j,a\in R\}\rangle$ （St(R)的下三角子群）

$T(I)=T(R)\cap \mathrm{St}(I)=\langle x_{ij}(I)\mid i<j\rangle$ （St(R)的一个子群）

$T'(I)=T'(R)\cap \mathrm{St}(I)=\langle x_{ij}(I)\mid i>j\rangle$ （St(R)的一个子群）

$\mathrm{U}(A)=(R/A)^{\cdot}=\{r\in R^{\cdot}\mid r\equiv 1 \pmod A\}$ （环 R 的相对单位(乘法)群）

$\mathrm{U}(R)=R^{\cdot}$ （R 的乘法群）

u. c. e. （群的泛中心扩张）

$v(R)=\langle (1+xy)(1+yx)^{-1}\mid x,y\in R,1+xy\in R^{\cdot}\}\rangle$ （$R^{\cdot}$ 的一个子群）

$V(R)=R^{\cdot}/v(R)$ （$R^{\cdot}$ 关于 $v(R)$的商群）

$\mathrm{w}=\bigcup\limits_{n=1}^{\infty}\mathrm{w}_n$ （St(R)的一个子群）

$\mathrm{w}_n=\mathrm{w}_n(R)$(由 $w_n(R^{\cdot})$生成的 $\mathrm{St}_n(R)$的子群）

【环】

$C(R)$ （环 R 的中心）

$C(X)$ （拓扑空间 X 上的连续函数环）

D 环 （Dieudonné 环，对一切 n，使 $R^{\cdot ab}\simeq \mathrm{GL}_n(R)$的环）

D_n 环 （使 $R^{\cdot ab}\simeq \mathrm{GL}_n(R)$的环）

D 环 （对一发 n 使 $V(R)\simeq \mathrm{GL}_n(R)$的环）

D'_n 环 （使 $V(R)\simeq \mathrm{GL}_n(R)$的环）

DD （Dedekind(整)环）

$\mathbb{F}_q=GF(q)$ （q 元有限域）

GE 环 （广义 Euclid 环）

IBN （不变基数环）

$J(R)$ （环 R 的 Jacobson 根）
K_0 环 （交换环的 K_0 群所成的环）
$\mathrm{lgD}(R)$ （环 R 的左整体维数）
$\mathrm{Max}R$ （环 R 的极大(理想)谱）
O_F （代数数域 F 的代数整元环）
PF （有限生成投射模都自由的环）
PID （主理想整环）
PSF （有限生成投射模都稳定自由的环）
PT 环 （投射平凡环，即幂等阵都可对角化的环）
$Q(R)$ （交换环 R 的全商环，整环的分式域）
RG （环 R 上关于群 G 的群环）
$R^{n\times n}$ （环 R 上的 n 阶矩阵环）
R_P （交换环 R 在素理想 P 的局部化）
SFF （稳定自由模都自由的环）
SGE （稳定 GE 环）
$\mathrm{Spec}(R)$ （环 R 的素(理想)谱）
$\mathrm{Sr}n$ （稳定度为 n 的环）
$S^{-1}R$（交换环 R 在乘法封闭集 S 的局部化）
UCP （有幺模列性质的环）

【其他】

det （行列式，Dieudonné 行列式，行列式映射）
$\mathrm{diag}(d_1,d_2,\cdots,d_n)$ （对角元为 $d_1,d_2,\cdots,d_n$ 的对角矩阵）
$d_v(x,y)=(-1)^{v(x)v(y)}x^{v(y)}/y^{v(x)}(\mathrm{mod}\ p)$ （F 上关于指数赋值 v 的驯符号，素数 $p>2$）
e_{ij}^a （对角元都是 1 且(i,j)位置为 a(其他元都为 0)的初等矩阵）
FI （分式理想集）
FI^* （可逆分式理想集）
h （类数）
h_n （n 次分圆域的类数）
$h_n^+=h_2(n)$ （n 次分圆域类数 h_n 的第二因子）
$h_n^-=h_1(n)$ （n 次分圆域的相对类数(h_n 的第一因子)）
$h_R=|\mathrm{Cl}(R)|$ （整环 R 的类数）
$H_{ij}(a,b)=x_{ji}(-b\alpha^{-1})x_{ij}(a)x_{ji}(b)x_{ij}(-a\beta^{-1})$ （Steinberg 群中有助于计算 K_2 群的元素，其中 $\alpha=1+ab\in R^*$，$\beta=1+ba\in R^*$）
$h_{ij}(u)=w_{ij}(u)w_{ij}(-1)$ （Steinberg 群中有用的一种元素）
I （单位矩阵）
I_n （n 阶单位矩阵）

I_X （代数系 X 上的恒等同态(映射)）

$N(a)$ （代数数域中元素 a 的范）

PFI （主分式理想集）

$T(a)$ （代数数域中元素 a 的迹）

$w_{ij}(u)=x_{ij}(u)x_{ji}(-u^{-1})x_{ij}(u)$ （Steinberg 群中有用的一种元素）

$x_{ij}(a)$ （Steinberg 群 St(R)的生成元）

$\Delta(\alpha_1,\cdots,\alpha_n)$ （n 次代数数域中 $\alpha_1,\cdots,\alpha_n$ 的判别式）

$\Delta(\sqrt{d})$ （二次数域$\mathbb{Q}(\sqrt{d})$(关于整基)的判别式）

χ （Euler 示性数）

$[P]$ （有限生成投射模 P 的稳定同构类）

$[A]$ （$A\in GL(R)$在 $K_1(R)$中的同余类）

$\|A\|=|O_F/A|$ （数域中 F 中代数整元环 O_F 的理想 A 的范）

$\|\alpha\|=|a_1|+\cdots+|a_n|$ （$\alpha=(a_1,\cdots,a_n)\in\mathbb{Z}^n$）

$(\frac{m}{p})$ （Legendre 记号）

$\oplus$ （模的直和，群的直积、直和，环的直积）

$\otimes$ （张量积）

$\simeq$ （同构）

$\{,\}$ （计算 K_2 群的 Steinberg 符号）

$(,)_2$ （$\mathbb{Q}(\mathbb{Q}^{\cdot}$)上的关于素数 2 的 Steinberg 符号）

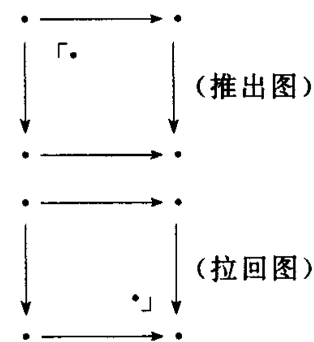
$(,)_p$ （$\mathbb{Q}(\mathbb{Q}^{\cdot}$)上关于素数 p 的 Steinberg 符号）

$(,)_\infty$ （Hilbert 符号）

[ ] （Mennicke 符号）

[,] （换位子记号，$[a,b]=aba^{-1}b^{-1}$或用作$[a,b]=ab-ba$）

$\langle,\rangle$ （计算 K_2 群的 Dennis-Stein 符号）



$\mathbb{C}$（复数域）

$\mathbb{N}$（非负整数加法半群）

$\mathbb{Q}$（有理数域）

$\mathbb{R}$（实数域）

$\mathbb{Z}$（整数环）